kaspersky

# Kaspersky Security Center 15.1 Windows

© 2026 AO Kaspersky Lab

# Contenido


Ayuda de Kaspersky Security Center 15.1

Novedades

Sobre Kaspersky Security Center

- Arquitectura
- Requisitos de hardware y software
  - Requisitos del Servidor de administración
  - Requisitos de Web Console
  - Requisitos de servidores móviles
  - Requisitos de la Consola de administración
  - Requisitos del Agente de red
- Aplicaciones y soluciones de Kaspersky compatibles
- Licencias y funciones de Kaspersky Security Center 15.1
- Acerca de la compatibilidad de los componentes de Kaspersky Security Center
- Comparación de Kaspersky Security Center: basado en Windows frente a basado en Linux
- Acerca de Kaspersky Security Center Cloud Console

Kaspersky Security Center 15.1

- Conceptos básicos
  - Servidor de administración
  - Jerarquía de Servidores de administración
  - Servidor de administración virtual
  - Servidor de dispositivos móviles
  - Servidor web
  - Agente de red
  - Grupos de administración
  - Dispositivo administrado
  - Dispositivo no asignado
  - Estación de trabajo del administrador
  - Complemento de administración
  - Complemento web de administración
  - Directivas
  - Perfiles de directivas
  - Tareas
  - Alcance de la tarea
  - Modo en que se relacionan las directivas y la configuración local de una aplicación
  - Punto de distribución
  - Puerta de enlace de conexión
- Escenario de instalación principal
- Puertos usados por Kaspersky Security Center
- Certificados para trabajar con Kaspersky Security Center
  - Acerca de los certificados de Kaspersky Security Center
  - Acerca del certificado del Servidor de administración
  - Requisitos para los certificados personalizados que se utilizan en Kaspersky Security Center
  - Procedimiento: Especificación del certificado del Servidor de administración personalizado

- Reemplazo del certificado del Servidor de administración mediante la utilidad klsetsrvcert
- Conexión de los Agentes de red al Servidor de administración mediante la utilidad klmover
- Volver a emitir el certificado del Servidor web

Esquemas del tráfico de datos y de los puertos utilizados
- Servidor de administración y dispositivos administrados en una LAN
- Servidor de administración principal en una LAN y dos Servidores de administración secundarios
- Servidor de administración en una LAN, dispositivos administrados en Internet, se usa un proxy inverso
- Servidor de administración en una LAN, dispositivos administrados en Internet, se usa una puerta de enlace de conexión
- Servidor de administración en una DMZ, dispositivos administrados en Internet
- Interacción entre los componentes de Kaspersky Security Center y las aplicaciones de seguridad: más información
  - Convenciones utilizadas en esquemas de interacción
  - Servidor de administración y DBMS
  - Servidor de administración y Consola de administración
  - Servidor de administración y dispositivo cliente: administración de la aplicación de seguridad
  - Actualización de software en un dispositivo cliente a través de un punto de distribución
  - Jerarquía de Servidores de administración: Servidor de administración principal y Servidor de administración secundario
  - Jerarquía de Servidores de administración con un Servidor de administración secundario en DMZ
  - Servidor de administración, una puerta de enlace de conexión en un segmento de red y un dispositivo cliente
  - Servidor de administración y dos dispositivos en DMZ: una puerta de enlace de conexión y un dispositivo cliente
  - Servidor de administración y Kaspersky Security Center Web Console
  - Activación y administración de la aplicación de seguridad en un dispositivo móvil

Prácticas recomendadas para el despliegue
- Guía para reforzar la seguridad
  - Instalación del Servidor de administración
  - Seguridad de la conexión
  - Cuentas y autenticación
  - Administrar la protección del Servidor de administración
  - Administración de la protección de dispositivos cliente
  - Configurar la protección para aplicaciones administradas
  - Mantenimiento del Servidor de administración
  - Transferencia de eventos a sistemas de terceros
  - Recomendaciones de seguridad para sistemas de información de terceros
  - Recomendaciones para usar las aplicaciones de seguridad de Kaspersky
- Preparativos para el despliegue
  - Planificación de la distribución de Kaspersky Security Center
    - Esquemas típicos para desplegar un sistema de protección
    - Información acerca de la planificación del despliegue de Kaspersky Security Center en la red de una organización
    - Selección de una estructura para la protección de una empresa
    - Configuraciones estándares de Kaspersky Security Center
      - Configuración estándar: oficina única
      - Configuración estándar: algunas oficinas a gran escala dirigidas por sus propios administradores
      - Configuración estándar: varias oficinas remotas pequeñas
    - Seleccionar un DBMS para el Servidor de administración
    - Configurar el servidor MariaDB x64 para trabajar con Kaspersky Security Center 15.1
    - Configurar el servidor MySQL x64 para que funcione con Kaspersky Security Center 15.1
    - Configurar el servidor PostgreSQL o Postgres Pro para trabajar con Kaspersky Security Center 15.1
    - Administración de dispositivos móviles con Kaspersky Endpoint Security para Android

Suministro de acceso a Internet al Servidor de administración
Acceso a Internet: Servidor de administración en una red local
Acceso a Internet: Servidor de administración en la zona desmilitarizada (DMZ)
Acceso a Internet: Agente de red en modo de puerta de enlace de conexión en DMZ
Acerca de los puntos de distribución
Aumentar el límite de descriptores de archivos para el servicio klnagent
Cálculo de la cantidad de puntos de distribución y su configuración
Jerarquía de Servidores de administración
Servidores de administración virtuales
Información sobre las limitaciones de Kaspersky Security Center
Carga de red
Despliegue inicial de la protección antivirus
Actualización inicial de las bases de datos antivirus
Sincronización de un cliente con el Servidor de administración
Actualización adicional de las bases de datos antivirus
Procesamiento de eventos de clientes mediante el Servidor de administración
Tráfico de 24 horas
Preparación para la administración de dispositivos móviles
Servidor de MDM para iOS
Configuración estándar: Kaspersky Device Management for iOS en una DMZ
Configuración estándar: Servidor de MDM para iOS en la red local de una organización
Administración de dispositivos móviles con Kaspersky Endpoint Security para Android
Información sobre el rendimiento del Servidor de administración
Limitaciones en la conexión a un Servidor de administración
Resultados de las pruebas de rendimiento del Servidor de administración
Resultados de las pruebas de rendimiento del servidor Proxy de KSN
Configuración de la red para interactuar con servicios externos
Despliegue del Agente de red y de la aplicación de seguridad
Despliegue inicial
Configuración de instaladores
Paquetes de instalación
Propiedades MSI y archivos de transformación
Despliegue con herramientas de terceros para la instalación remota de aplicaciones
Acerca de las tareas de instalación remota en Kaspersky Security Center
Despliegue mediante la captura y copia de la imagen de un dispositivo
Copia incorrecta de una imagen del disco duro
Despliegue mediante directivas de grupo de Microsoft Windows
Despliegue forzado con la tarea de instalación remota de Kaspersky Security Center
Ejecución de paquetes independientes creados por Kaspersky Security Center
Opciones para la instalación manual de aplicaciones
Crear un archivo MST
Instalación remota de aplicaciones en dispositivos en los que se encuentra instalado el Agente de red
Opciones para controlar el reinicio de los dispositivos en la tarea de instalación remota
Conveniencia de actualizar las bases de datos en el paquete de instalación de una aplicación de seguridad
Utilización de herramientas para la instalación remota de aplicaciones en Kaspersky Security Center para ejecutar archivos ejecutables relevantes en dispositivos administrados
Supervisión del despliegue

Configuración de instaladores
Información general
Instalación en modo silencioso (con un archivo de respuesta)
Instalación del Agente de red en modo silencioso (sin un archivo de respuesta)
Configuración de instalación parcial a través de setup.exe
Parámetros de instalación del Servidor de administración
Agente de red: parámetros de instalación
Infraestructura virtual
Sugerencias sobre la reducción de la carga en máquinas virtuales
Compatibilidad con máquinas virtuales dinámicas
Soporte de copia de máquinas virtuales
Soporte de reversión del sistema de archivos para dispositivos con Agente de red
Instalación local de aplicaciones
Instalación local del Agente de red
Instalación del Agente de red en modo silencioso
Instalación del Agente de red para Linux en modo silencioso (con un archivo de respuestas)
Preparación de un dispositivo que ejecuta Astra Linux en el modo de entorno de software cerrado para la instalación del Agente de red
Instalación del Agente de red para Linux en modo interactivo
Instalación local del complemento de administración de aplicaciones
Instalación de aplicaciones en modo no interactivo
Instalación de aplicaciones con paquetes independientes
Ajustes del paquete de instalación del Agente de red
Ver la Política de privacidad
Despliegue de los sistemas de administración de dispositivos móviles
Despliegue de un sistema de administración para el protocolo MDM para iOS
Instalación del Servidor de MDM para iOS
Instalación del Servidor de MDM para iOS en modo no interactivo
Escenarios de despliegue del Servidor de MDM para iOS
Esquema de despliegue simplificado
Esquema de despliegue para usar la delegación restringida de Kerberos (KCD)
Recepción de un certificado de APNs
Renovación de un certificado de APNs
Configuración de un certificado de reserva de Servidor de MDM para iOS
Instalación de un certificado de APNs en un Servidor de MDM para iOS
Configuración del acceso al servicio de Apple Push Notification
Emisión e instalación de un certificado compartido en un dispositivo móvil
Incorporación de un dispositivo KES a la lista de dispositivos administrados
Conexión de dispositivos KES al Servidor de administración
Conexión directa de dispositivos al Servidor de administración
Esquema para conectar dispositivos KES al Servidor en el que se usa la delegación restringida de Kerberos (KCD)
Usar Firebase Cloud Messaging
Integración con una infraestructura de claves públicas
Servidor web de Kaspersky Security Center
Instalación de Kaspersky Security Center
Preparación para la instalación
Cuentas para trabajar con el DBMS

Configurar las cuentas para trabajar con SQL Server (autenticación de Windows)
Configurar las cuentas para trabajar con SQL Server (autenticación de SQL Server)
Configurar las cuentas para trabajar con MySQL y MariaDB
Mover datos desde un espacio de tabla compartido a un espacio de tabla por archivo en un DBMS MySQL o MariaDB
Configurar las cuentas para trabajar con PostgreSQL y Postgres Pro
Escenario: autenticación de Microsoft SQL Server
Escenario: autenticación del servidor MySQL
Escenario: autenticación del servidor PostgreSQL
Recomendaciones sobre la instalación del Servidor de administración
Creación de cuentas para los servicios del Servidor de administración en un clúster de conmutación por error
Definición de una carpeta compartida
Instalación remota con herramientas del Servidor de administración a través de directivas de grupo de Active Directory
Instalación remota a través de la distribución de la ruta de UNC a un paquete independiente
Actualización desde la carpeta compartida del Servidor de administración
Instalación de imágenes de los sistemas operativos
Especificación de la dirección del Servidor de administración
Instalación estándar
Paso 1. Revisar el Contrato de licencia y la Política de privacidad
Paso 2. Seleccionar el método de instalación
Paso 3. Instalación de Kaspersky Security Center Web Console
Paso 4. Seleccionar el tamaño de la red
Paso 5. Seleccionar una base de datos
Paso 6. Configurar el Servidor SQL
Paso 7. Seleccionar el modo de autenticación
Paso 8. Desempaquetar e instalar archivos en el disco duro
Instalación personalizada
Paso 1. Revisar el Contrato de licencia y la Política de privacidad
Paso 2. Seleccionar el método de instalación
Paso 3. Seleccionar los componentes a instalar
Paso 4. Instalación de Kaspersky Security Center Web Console
Paso 5. Seleccionar el tamaño de la red
Paso 6. Seleccionar una base de datos
Paso 7. Configurar el Servidor SQL
Paso 8. Seleccionar el modo de autenticación
Paso 9. Seleccionar la cuenta para iniciar el Servidor de administración
Paso 10. Selección de una cuenta para ejecutar los servicios de Kaspersky Security Center
Paso 11. Seleccionar una carpeta compartida
Paso 12. Configurar la conexión al Servidor de administración
Paso 13. Definir la dirección del Servidor de administración
Paso 14. Dirección del Servidor de administración para la conexión de dispositivos móviles
Paso 15. Seleccionar complementos de administración de aplicaciones
Paso 16. Desempaquetar e instalar archivos en el disco duro
Despliegue del clúster de conmutación por error de Kaspersky Security Center
Escenario: Despliegue de un clúster de conmutación por error de Kaspersky Security Center
Sobre el clúster de conmutación por error de Kaspersky Security Center
Preparación de un servidor de archivos para un clúster de conmutación por error de Kaspersky Security Center
Preparación de nodos para un clúster de conmutación por error de Kaspersky Security Center

Instalación de Kaspersky Security Center en los nodos del clúster de conmutación por error de Kaspersky Security Center
Iniciar y detener nodos del clúster manualmente
Instalación del Servidor de administración en un clúster de conmutación por error de Windows Server
Paso 1. Revisar el Contrato de licencia y la Política de privacidad
Paso 2. Seleccionar el tipo de instalación en un clúster
Paso 3. Especificar el nombre del Servidor de administración virtual
Paso 4. Especificar los datos de la red del Servidor de administración virtual
Paso 5. Especificar un grupo de clústeres
Paso 6. Seleccionar un almacenamiento de datos de clúster
Paso 7. Especificar una cuenta para realizar la instalación remota
Paso 8. Seleccionar los componentes a instalar
Paso 9. Seleccionar el tamaño de la red
Paso 10. Seleccionar una base de datos
Paso 11. Configurar el Servidor SQL
Paso 12. Seleccionar el modo de autenticación
Paso 13. Seleccionar la cuenta para iniciar el Servidor de administración
Paso 14. Selección de una cuenta para ejecutar los servicios de Kaspersky Security Center
Paso 15. Seleccionar una carpeta compartida
Paso 16. Configurar la conexión al Servidor de administración
Paso 17. Definir la dirección del Servidor de administración
Paso 18. Dirección del Servidor de administración para la conexión de dispositivos móviles
Paso 19. Desempaquetar e instalar archivos en el disco duro
Instalación del Servidor de administración en modo no interactivo
Instalación de la Consola de administración en la estación de trabajo del administrador
Cambios en el sistema después de la instalación de Kaspersky Security Center
Eliminando la aplicación
Acerca de las actualizaciones de versión en Kaspersky Security Center
Actualización de Kaspersky Security Center desde una versión anterior
Actualización de Kaspersky Security Center en los nodos del clúster de conmutación por error de Kaspersky Security Center
Actualizar Kaspersky Security Center en los nodos de un clúster de conmutación por error de Microsoft
Configuración inicial de Kaspersky Security Center
Guía para reforzar la seguridad
Asistente de inicio rápido del Servidor de administración
Acerca del asistente de inicio rápido
Iniciar el Asistente de inicio rápido del Servidor de administración
Paso 1. Configuración de un servidor proxy
Paso 2. Selección del método de activación de la aplicación
Paso 3. Selección de las áreas de protección y sistemas operativos
Paso 4. Selección de complementos para las aplicaciones administradas
Paso 5. Descarga de paquetes de distribución y creación de paquetes de instalación
Paso 6. Configuración del uso de Kaspersky Security Network
Paso 7. Configuración de notificaciones por correo electrónico
Paso 8. Configuración de administración de actualizaciones
Paso 9. Creación de una configuración de protección inicial
Paso 10. Conexión de dispositivos móviles

Paso 11. Descargar actualizaciones
Paso 12. Descubrimiento de dispositivos
Paso 13. Cierre del asistente de inicio rápido
Configuración de la conexión de la Consola de administración al Servidor de administración
Configuración de las opciones de acceso a Internet para el Servidor de administración
Conexión de dispositivos fuera de la oficina
Escenario: conexión de dispositivos fuera de la oficina mediante una puerta de enlace de conexión
Escenario: Conectar dispositivos fuera de la oficina mediante un Servidor de administración secundario en la DMZ
Acerca de la conexión de dispositivos fuera de la oficina
Conectar dispositivos de escritorio externos al Servidor de administración
Acerca de los perfiles de conexión para los usuarios fuera de la oficina
Creación de un perfil de conexión para usuarios fuera de la oficina
Acerca de cambiar el Agente de red a otros Servidores de administración
Creación de una regla de conmutación del Agente de red por ubicación de red
Notificación de eventos
Configuración de la notificación de eventos
Notificaciones de prueba
Notificaciones de eventos que se muestran al ejecutar un archivo ejecutable
Cifrar la comunicación con TLS
Configuración de la interfaz
Descubrimiento de dispositivos conectados a la red
Escenario: Descubrir dispositivos conectados a la red
Dispositivos no asignados
Descubrimiento de dispositivos
Sondeo de la red de Windows
Sondeo de Active Directory
Sondeo de intervalos IP
Sondeo con Zeroconf
Trabajar con dominios de Windows. Ver y cambiar la configuración de dominio
Configuración de reglas de retención para dispositivos no asignados
Trabajar con rangos IP
Crear un rango IP
Ver y modificar la configuración del rango IP
Trabajar con los grupos de Active Directory. Ver y cambiar la configuración de grupo
Crear reglas para mover dispositivos a grupos de administración automáticamente
Usar el modo dinámico para la Infraestructura de escritorio virtual (VDI) en los dispositivos cliente
Habilitación del modo dinámico de la Infraestructura de escritorio virtual (VDI) en las propiedades de un paquete de instalación para el Agente de red
Buscar dispositivos que formen parte de la VDI
Mover los dispositivos que forman parte de la VDI a un grupo de administración
Inventario de equipos
Agregar información sobre los dispositivos nuevos
Configurar criterios usados para los dispositivos de empresa
Configuración de campos personalizados
Licencias
Eventos sobre límites de licencia superados
Sobre licencias

Acerca de la licencia
Acerca del Contrato de licencia de usuario final
Acerca del certificado de licencia
Acerca de la clave de licencia
Acerca del archivo de clave
Acerca de la suscripción
Acerca del código de activación
Revocar la aceptación de un Contrato de licencia de usuario final
Sobre la provisión de datos
Opciones de licencias de Kaspersky Security Center
Funciones de licencia de Kaspersky Security Center y aplicaciones administradas
Aplicaciones de Kaspersky. Despliegue centralizado
Reemplazo de aplicaciones de seguridad de terceros
Instalar aplicaciones mediante la tarea de instalación remota
Instalar una aplicación en los dispositivos seleccionados
Instalar una aplicación en dispositivos cliente del grupo de administración
Instalar una aplicación mediante las directivas de grupo de Active Directory
Instalación remota de aplicaciones en dispositivos macOS
Instalar aplicaciones en los Servidores de administración secundarios
Instalar aplicaciones mediante el Asistente de instalación remota
Trabajar con los complementos de administración
Ver un informe sobre el despliegue de la protección
Eliminar aplicaciones de manera remota
Eliminación remota de una aplicación de dispositivos cliente del grupo de administración
Eliminación remota de una aplicación de dispositivos seleccionados
Trabajar con paquetes de instalación
Creación del paquete de instalación
Creación de paquetes de instalación independientes
Crear un paquete de instalación personalizado
Ver y editar propiedades de paquetes de instalación personalizada
Obtención del paquete de instalación del Agente de red del kit de distribución de Kaspersky Security Center
Distribución de paquetes de instalación a servidores de administración secundarios
Distribución de paquetes de instalación a través de los puntos de distribución
Transferir los resultados de la instalación de aplicaciones a Kaspersky Security Center
Definición de la dirección del servidor proxy de KSN para los paquetes de instalación
Recibir versiones actualizadas de las aplicaciones
Preparar un dispositivo Windows para la instalación remota
Preparación de un dispositivo Linux e instalación del Agente de red en un dispositivo Linux de forma remota
Preparación de un dispositivo que ejecuta SUSE Linux Enterprise Server 15 para la instalación del Agente de red
Preparación de un dispositivo de macOS para instalación remota de Agente de red
Aplicaciones de Kaspersky: licencias y activación
Licencias de aplicaciones administradas
Visualización de información sobre las claves de licencia en uso
Agregar una clave de licencia al repositorio del Servidor de administración
Eliminar una clave de licencia del Servidor de administración
Distribución de claves de licencia a dispositivos cliente
Distribución automática de una clave de licencia

Crear y ver un informe de uso de claves de licencia
Ver información sobre las claves de licencia de la aplicación
Exportación de un archivo de clave de licencia
Configurar la protección de la red
Procedimiento: Configurar la protección de la red
Configuración y propagación de directivas: enfoque centrado en el dispositivo
Acerca de la administración de la seguridad centrada en el dispositivo y centrada en el usuario
Configuración manual de la directiva de Kaspersky Endpoint Security
Configuración de la directiva en la sección Protección avanzada contra amenazas
Configuración de la directiva en la sección Protección básica contra amenazas
Configuración de la directiva en la sección Configuración general
Configuración de la directiva en la sección Configuración de eventos
Configuración manual de la tarea de grupo para actualizar Kaspersky Endpoint Security
Instalación manual de la tarea de grupo para analizar un dispositivo con Kaspersky Endpoint Security
Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas
Configuración manual de la tarea de grupo para la instalación de actualizaciones y la reparación de vulnerabilidades
Configuración del número máximo de eventos en el repositorio de eventos
Configurar el período máximo de almacenamiento para la información sobre las vulnerabilidades reparadas
Administración de tareas
Crear una tarea
Crear una tarea del Servidor de administración
Crear una tarea para dispositivos específicos
Crear una tarea local
Mostrar una tarea de grupo heredada en el espacio de trabajo de un grupo anidado
Encender dispositivos automáticamente antes de iniciar una tarea
Apagar el dispositivo automáticamente una vez que se haya completado la tarea
Limitar el tiempo de ejecución de la tarea
Exportar una tarea
Importar una tarea
Convertir tareas
Iniciar y detener una tarea manualmente
Pausar y reanudar una tarea manualmente
Supervisar la ejecución de tareas
Ver resultados de la ejecución de tareas almacenados en el Servidor de administración
Configurar el filtrado de información sobre resultados de la ejecución de tareas
Modificar una tarea. Reversión de cambios
Comparación de tareas
Cuentas para iniciar tareas
Exportar el historial de ejecución de tareas
Asistente para cambiar contraseñas de tareas
Paso 1. Especificar credenciales
Paso 2. Seleccionar una acción para realizar
Paso 3. Ver los resultados
Creación de una jerarquía de grupos de administración subordinados a un Servidor de administración virtual.
Directivas y perfiles de directivas
Jerarquía de directivas, usando perfiles de directivas
Jerarquía de directivas

Perfiles de directivas
Herencia de configuración de la directiva
Administración de directivas
Crear una directiva
Mostrar directiva heredada en un subgrupo
Activar una directiva
Activar una directiva automáticamente ante un brote de virus
Aplicación de una directiva fuera de la oficina
Modificación de una directiva. Reversión de cambios
Comparación de directivas
Ver el gráfico de distribución de una directiva
Eliminar una directiva
Copiar una directiva
Exportación de una directiva
Importación de una directiva
Convertir directivas
Administración de perfiles de directivas
Crear un perfil de directiva
Modificar un perfil de directiva
Eliminar un perfil de directiva
Crear una regla de activación para un perfil de directiva
Reglas de movimiento de dispositivos
Clonación de reglas de movimiento de dispositivos
Categorización del software
Requisitos previos para instalar aplicaciones en dispositivos de una organización cliente
Ver y modificar la configuración local de la aplicación
Actualización de Kaspersky Security Center y de las aplicaciones administradas
Procedimiento: actualización regular de bases de datos y aplicaciones de Kaspersky
Acerca de la actualización de las bases de datos, los módulos de software y las aplicaciones de Kaspersky
Acerca de la utilización de archivos diff para actualizar las bases de datos y los módulos de software de Kaspersky
Habilitación de la función de descarga de archivos diff
Crear la tarea para descargar actualizaciones en el repositorio del Servidor de administración
Creación de la tarea Descargar actualizaciones en los repositorios de los puntos de distribución
Configuración de la tarea del Servidor de administración Descargar actualizaciones en el repositorio
Comprobar actualizaciones descargadas
Configurar las directivas de prueba y tareas auxiliares
Ver actualizaciones descargadas
Instalación automática de actualizaciones de Kaspersky Endpoint Security en los dispositivos
Modelo de descarga de actualizaciones sin conexión
Habilitación y deshabilitación del modelo de descarga de actualizaciones sin conexión
Actualización automática y parches para componentes de Kaspersky Security Center
Habilitación y deshabilitación de actualizaciones automáticas y parches para componentes de Kaspersky Security Center
Distribución automática de las actualizaciones
Distribución automática de actualizaciones a dispositivos cliente
Distribución automática de actualizaciones a Servidores de administración secundarios
Asignar puntos de distribución automáticamente
Asignación manual de un punto de distribución a un dispositivo

Eliminación de un dispositivo de la lista de puntos de distribución
Descarga de actualizaciones por puntos de distribución
Eliminación de actualizaciones de software desde el repositorio
Instalación de parches para una aplicación de Kaspersky en modo de clúster
Administración de aplicaciones de terceros en dispositivos cliente
Acerca de las aplicaciones de terceros
Instalación de actualizaciones para software de terceros
Procedimiento: Actualización de software de terceros
Visualización de información sobre actualizaciones disponibles para aplicaciones de terceros
Aprobar y rechazar actualizaciones de software
Sincronización de las actualizaciones de Windows Update con el Servidor de administración
Paso 1. Definir la reducción de tráfico
Paso 2. Aplicaciones
Paso 3. Categorías de actualizaciones
Paso 4. Idiomas de actualizaciones
Paso 5. Selección de una cuenta para iniciar la tarea
Paso 6. Configuración de una programación de inicio para la tarea
Paso 7. Definición del nombre de la tarea
Paso 8. Completar creación de la tarea
Instalación de actualizaciones en dispositivos manualmente
Configuración de actualizaciones de Windows en una directiva del Agente de red
Reparación de vulnerabilidades en el software de terceros
Procedimiento: búsqueda y reparación de vulnerabilidades de software de terceros
Acerca de la búsqueda y reparación de vulnerabilidades de software
Consulta de información sobre las vulnerabilidades de software
Ver estadísticas de las vulnerabilidades presentes en los dispositivos administrados
Análisis de aplicaciones en busca de vulnerabilidades
Reparación de vulnerabilidades en las aplicaciones
Reparar vulnerabilidades en una red aislada
Procedimiento: reparar vulnerabilidades en el software de terceros
Acerca de la reparación de vulnerabilidades en el software de terceros en una red aislada
Configurar el Servidor de administración con acceso a Internet para reparar vulnerabilidades en una red aislada
Configurar los servidores de administración aislados para reparar vulnerabilidades en una red aislada
Transmitir parches e instalar actualizaciones en una red aislada
Deshabilitar la opción para transmitir parches e instalar actualizaciones en una red aislada
Ignorar vulnerabilidades de software
Selección de soluciones de usuario para vulnerabilidades de software de terceros
Reglas para la instalación de actualizaciones
Grupos de aplicaciones
Uso de Control de aplicaciones para administrar archivos ejecutables
Obtención y visualización de una lista de archivos ejecutables almacenados en los dispositivos cliente
Creación de categorías de aplicaciones para las directivas de Kaspersky Endpoint Security para Windows
Creación de una categoría de aplicaciones con contenido agregado manualmente
Crear una categoría de aplicaciones con archivos ejecutables de dispositivos específicos
Creación de una categoría de aplicaciones que incluya archivos ejecutables de una carpeta específica
Agregar archivos ejecutables vinculados a eventos a una categoría de aplicaciones
Configuración de la administración de inicio de aplicaciones en dispositivos cliente

Visualización de los resultados del análisis estático de las reglas de inicio aplicadas a los archivos ejecutables
Consulta del registro de aplicaciones
Modificación de la hora de inicio del inventariado de software
Acerca de la administración de claves de licencia de aplicaciones de terceros
Crear grupos de aplicaciones con licencia
Administración de claves de licencia para grupos de aplicaciones con licencia
Inventario de archivos ejecutables
Visualización de información sobre archivos ejecutables
Supervisión e informes
Procedimiento: Supervisión y generación de informes
Controlar los semáforos y los eventos registrados en la Consola de Administración
Trabajo con informes, estadísticas y notificaciones
Trabajar con informes
Crear una plantilla de informe
Ver y editar las propiedades de una plantilla de informe
Formato de filtro extendido en plantillas de informes
Conversión del filtro al formato extendido
Configuración del filtro extendido
Crear y ver un informe
Guardar un informe
Crear una tarea de entrega de informes
Paso 1. Selección del tipo de tarea
Paso 2. Selección del tipo de informe
Paso 3. Acciones en un informe
Paso 4. Selección de una cuenta para iniciar la tarea
Paso 5. Configuración de una programación de tarea
Paso 6. Definición del nombre de la tarea
Paso 7. Completar creación de la tarea
Administración de estadísticas
Configuración de la notificación de eventos
Creación de un certificado para un servidor SMTP
Selecciones de eventos
Ver una selección de eventos
Personalizar una selección de eventos
Crear una selección de eventos
Exportar una selección de eventos a un archivo de texto
Eliminar eventos de una selección
Agregar aplicaciones a las exclusiones mediante solicitudes de los usuarios
Selecciones de dispositivos
Visualización de una selección de dispositivos
Configurar una selección de dispositivos
Exportar la configuración de una selección de dispositivos a un archivo
Crear una selección de dispositivos
Crear una selección de dispositivos según la configuración importada
Eliminación de dispositivos de los grupos de administración en una selección
Supervisión de instalación y desinstalación de aplicaciones
Eventos de los componentes de Kaspersky Security Center

Estructura de datos utilizada para describir los tipos de eventos
Eventos del Servidor de administración
Eventos del Servidor de administración: nivel Crítico
Eventos del Servidor de administración: nivel Error funcional
Eventos del Servidor de administración: nivel Advertencia
Eventos del Servidor de administración: nivel Información
Eventos del Agente de red
Eventos del Agente de red: nivel Error funcional
Eventos del Agente de red: nivel Advertencia
Eventos del Agente de red: nivel Información
Eventos del Servidor de MDM para iOS
Eventos de errores funcionales del Servidor de MDM para iOS
Eventos de advertencia del servidor de MDM para iOS
Eventos informativos del servidor de MDM para iOS
Bloquear eventos frecuentes
Acerca del bloqueo de eventos frecuentes
Administrar el bloqueo de eventos frecuentes
Eliminar el bloqueo de eventos frecuentes
Exportar una lista de eventos frecuentes en un archivo
Controlar los cambios en el estado de las máquinas virtuales
Supervisar el estado de la protección antivirus utilizando información del registro del sistema
Ver y configurar las acciones para dispositivos inactivos
Dejar de recibir las novedades de Kaspersky
Ajuste de puntos de distribución y puertas de enlace de conexión
Configuración estándar de puntos de distribución: oficina única
Configuración estándar de puntos de distribución: varias oficinas remotas pequeñas
Designación de un dispositivo administrado como un punto de distribución
Conexión de un dispositivo Linux como una puerta de enlace en la zona desmilitarizada
Conexión de un dispositivo Linux al Servidor de administración a través de una puerta de enlace de conexión
Agregar una puerta de enlace de conexión ubicada en una DMZ como punto de distribución
Asignar puntos de distribución automáticamente
Acerca de la instalación local del Agente de red en un dispositivo seleccionado como punto de distribución
Acerca del uso de un punto de distribución como puerta de enlace de conexión
Agregar rangos de IP a la lista de rangos sondeados por un punto de distribución
Uso de un punto de distribución como servidor push
Otro trabajo de rutina
Administración de los Servidores de administración
Creación de una jerarquía de servidores de administración: agregar un Servidor de administración secundario
Conexión a un Servidor de administración y alternancia entre Servidores de administración
Permisos de acceso al Servidor de administración y sus objetos
Condiciones de conexión a un Servidor de administración a través de Internet
Conexión cifrada con un Servidor de administración
Autenticación del Servidor de administración cuando un dispositivo se conecta
Autenticación del Servidor de administración durante la conexión de la Consola de administración
Configuración de una lista de admitidos de direcciones IP para conectarse al Servidor de administración
Usar la utilidad klscflag para cerrar el puerto 13291
Desconexión de un Servidor de administración

- Agregar un Servidor de administración al árbol de consola
- Eliminación de un Servidor de administración del árbol de consola
- Agregar un Servidor de administración virtual al árbol de consola
- Cambio de una cuenta de servicio del Servidor de administración Utilidad klsrvswch
- Cambio de las credenciales de DBMS
- Cambiar la carpeta compartida del Servidor de administración
- Resolución de problemas con los nodos del Servidor de administración
- Visualización y modificación de la configuración de un Servidor de administración
  - Ajuste de la configuración general del Servidor de administración
  - Configuración de la interfaz de la Consola de administración
  - Almacenamiento y procesamiento de eventos en el Servidor de administración
  - Visualización del registro de conexiones al Servidor de administración
  - Control de brotes de virus
  - Límite de tráfico
  - Configuración del Servidor web
  - Trabajar con usuarios internos
- Copia de seguridad y restauración de la configuración del Servidor de administración
  - Uso de una instantánea del sistema de archivos para reducir la duración de la copia de seguridad
  - Un dispositivo con el Servidor de administración es inoperable
  - La configuración del Servidor de administración o la base de datos es corrupta
- Copia de seguridad y restauración de los datos del Servidor de administración
  - Tarea Copia de seguridad de los datos del Servidor de administración
  - Utilidad de copia de seguridad y recuperación de datos (klbackup)
  - Copia de seguridad y recuperación de datos en modo interactivo
  - Copia de seguridad y recuperación de datos en modo no interactivo
  - Usar la utilidad klbackup para ceder el control de los dispositivos administrados a otro Servidor de administración
  - Cómo hacer copias de seguridad y restaurar datos del Servidor de administración si se usa MySQL o MariaDB
  - Optimizar la copia de seguridad y restauración de los datos del Servidor de administración
- Mover el Servidor de administración a otro dispositivo
- Evitar conflictos entre varios Servidores de administración

Administrar grupos de administración
- Creación de grupos de administración
- Traslado de grupos de administración
- Eliminación de grupos de administración
- Creación automática de la estructura de grupos de administración
- Instalación automática de aplicaciones en dispositivos de un grupo de administración

Administración de dispositivos cliente
- Conexión de dispositivos cliente al Servidor de administración
- Conexión manual de un dispositivo cliente al Servidor de administración. Utilidad klmover
- Creación de un túnel de conexión entre un dispositivo cliente y el Servidor de administración
- Conexión remota al escritorio de un dispositivo cliente
  - Conexión a dispositivos cliente de Windows
  - Conexión a dispositivos cliente macOS
- Conectarse a un dispositivo a través de Windows Desktop Sharing
- Configurar el reinicio de un dispositivo cliente
- Auditoría de acciones en un dispositivo cliente remoto
- Comprobación de la conexión entre un dispositivo cliente y el Servidor de administración

Comprobación automática de la conexión entre un dispositivo cliente y el Servidor de administración
Comprobación manual de la conexión entre un dispositivo cliente y el Servidor de administración. Utilidad klnagchk
Acerca de la comprobación de la hora de conexión entre un dispositivo y el Servidor de administración
Identificación de dispositivos cliente en el Servidor de administración
Mover dispositivos a un grupo de administración
Cambiar los dispositivos cliente de Servidor de administración
Mover dispositivos conectados a un Servidor de administración mediante puertas de enlace de conexión a otro Servidor de administración
Clústeres y conjuntos de servidores
Encendido, apagado y reinicio remoto de dispositivos cliente
Acerca del uso de la conexión continua entre un dispositivo administrado y el Servidor de administración
Acerca de la sincronización forzada
Sobre la programación de conexión
Envío de mensajes a usuarios de dispositivos
Administración de Kaspersky Security for Virtualization
Configurar cambios de estado para los dispositivos
Etiquetado de dispositivos y visualización de etiquetas asignadas
Etiquetado automático de dispositivos
Visualización y configuración de etiquetas asignadas a un dispositivo
Diagnóstico remoto de dispositivos cliente. Utilidad de diagnóstico remoto de Kaspersky Security Center
Conexión de la utilidad de diagnóstico remoto a un dispositivo cliente
Crear un archivo de volcado para una aplicación
Activar y desactivar el seguimiento, descargar el archivo de seguimiento
Descargar la configuración de las aplicaciones
Descargar registros de eventos
Descarga de varios elementos de información de diagnóstico
Inicio de los diagnósticos y descarga de los resultados
Iniciar, detener y reiniciar aplicaciones
Dispositivos con protección de UEFI
Configuración de un dispositivo administrado
Ajustes generales de una directiva
Ajustes de la directiva del Agente de red
Administrar cuentas de usuario
Trabajar con cuentas de usuario
Agregar una cuenta de un usuario interno
Editar una cuenta de un usuario interno
Cambiar el número de intentos de entrada de contraseña permitidos
Configurar la verificación de que el nombre de un usuario interno sea único
Agregar un grupo de seguridad
Agregar un usuario a un grupo
Configurar los derechos de acceso a las funciones de la aplicación. Control de acceso basado en roles
Derechos de acceso a las funciones de la aplicación
Roles de usuario predefinidos
Agregar un rol de usuario
Asignación de un rol a un usuario o a un grupo de seguridad
Asignación de permisos a usuarios y grupos
Propagación de roles de usuario a Servidores de administración secundarios

- Asignar al usuario como propietario del dispositivo
- Enviar mensajes a los usuarios
- Ver la lista de dispositivos móviles de los usuarios
- Instalar un certificado para un usuario
- Ver la lista de certificados emitidos para un usuario
- Acerca del administrador del Servidor de administración virtual

Instalación remota de sistemas operativos y aplicaciones

- Crear imágenes de sistemas operativos
- Instalación de imágenes de los sistemas operativos
- Configurar la dirección del servidor proxy de KSN
- Agregar controladores para el Entorno de preinstalación de Windows (WinPE)
- Agregar controladores a un paquete de instalación con una imagen del sistema operativo
- Configurar la utilidad sysprep.exe
- Instalar sistemas operativos en dispositivos nuevos de la red
- Instalar sistemas operativos en dispositivos cliente
- Crear paquetes de instalación de aplicaciones
- Emitir un certificado para paquetes de instalación de aplicaciones
- Instalar aplicaciones en dispositivos cliente

Administración de revisiones de objetos

- Acerca de las revisiones de objetos
- Visualización de la sección Historial de revisión
- Comparación de revisiones de objetos
- Configuración del plazo de almacenamiento de revisiones de objetos y de información de objetos eliminados
- Visualización de una revisión de objetos
- Almacenamiento de una revisión de objetos en un archivo
- Reversión de cambios
- Agregar una descripción a una revisión

Eliminación de objetos

- Eliminar objeto
- Visualización de información sobre los objetos eliminados
- Eliminar objetos permanentemente de la lista de objetos eliminados

Administración de dispositivos móviles

- Escenario: Despliegue de la característica Administración de dispositivos móviles
- Acerca de la directiva de grupo para la administración de dispositivos MDM con iOS
- Habilitar Administración de dispositivos móviles
- Modificar la configuración de administración de dispositivos móviles
- Deshabilitar la administración de dispositivos móviles
- Trabajar con comandos para dispositivos móviles
  - Comandos para la administración de dispositivos móviles
  - Usar Firebase Cloud Messaging
  - Enviar comandos
  - Ver los estados de los comandos en el registro de comandos
- Trabajar con certificados de dispositivos móviles
  - Iniciar el Asistente de instalación de certificados
  - Paso 1. Selección del tipo de certificado
  - Paso 2. Selección del tipo de dispositivo
  - Paso 3. Selección de un usuario

Paso 4. Selección del origen del certificado
Paso 5. Asignación de una etiqueta al certificado
Paso 6. Especificación de configuración de publicación de certificados
Paso 7. Selección del método de notificación al usuario
Paso 8. Generación del certificado
Configuración de las reglas de emisión de certificados
Integración con la infraestructura de claves públicas
Habilitar la compatibilidad con la delegación restringida de Kerberos
Adición de dispositivos móviles iOS a la lista de dispositivos administrados
Incorporar dispositivos móviles Android a la lista de dispositivos administrados
Administración de dispositivos MDM con iOS
Firmar un perfil de MDM para iOS mediante un certificado
Agregar un perfil de configuración
Instalación de un perfil de configuración en un dispositivo
Eliminación de un perfil de configuración de un dispositivo
Adición de un dispositivo nuevo al publicar un enlace a un perfil
Adición de un dispositivo nuevo a través de instalación del perfil por el administrador
Adición de un perfil de aprovisionamiento
Instalación de un perfil de aprovisionamiento en un dispositivo
Eliminación de un perfil de aprovisionamiento de un dispositivo
Agregar una aplicación administrada
Instalar una app en un dispositivo móvil
Eliminar una app de un dispositivo
Configuración de roaming en un dispositivo móvil MDM con iOS
Ver la información acerca de un dispositivo MDM con iOS
Desconectar de la administración un dispositivo MDM con iOS
Envío de comandos a un dispositivo
Comprobación del estado de ejecución de comandos enviada
Administración de dispositivos KES
Crear un paquete de aplicaciones móviles para dispositivos KES
Habilitar la autenticación basada en certificados para dispositivos KES
Ver la información acerca de un dispositivo KES
Desconectar de la administración un dispositivo KES
Protección y cifrado de datos
Ver la lista de dispositivos cifrados
Ver la lista de eventos de cifrado
Exportar la lista de eventos de cifrado en un archivo de texto
Crear y ver informes de cifrado
Transmisión de claves de cifrado entre Servidores de administración
Repositorios de datos
Exportar una lista de objetos de repositorio a un archivo de texto
Paquetes de instalación
Principales estados de los archivos en el repositorio
Activación de reglas en modo Aprendizaje inteligente
Cómo ver la lista de detecciones realizadas con las reglas del Control de anomalías adaptativo
Adición de exclusiones para las reglas del Control de anomalías adaptativo
Paso 1. Seleccionar la aplicación

Paso 2. La selección de la directiva (directivas)
Paso 3. Procesamiento de la directiva (directivas)
Cuarentena y Copia de seguridad
Habilitar la administración remota para archivos en repositorios
Visualizar propiedades de un archivo colocado en repositorio
Eliminar archivos de los repositorios
Restaurar archivos desde los repositorios
Guardar un archivo desde los repositorios al disco
Escaneo de archivos en Cuarentena
Amenazas activas
Desinfección de un archivo no procesado
Guardar un archivo no procesado en disco
Eliminar archivos desde la carpeta "Amenazas activas"
Kaspersky Security Network (KSN)
Acerca de KSN
Configuración del acceso a Kaspersky Security Network
Habilitar y deshabilitar KSN
Ver la Declaración de KSN aceptada
Ver las estadísticas del servidor proxy de KSN
Aceptar una Declaración de KSN actualizada
Mejor protección con Kaspersky Security Network
Verificar si el punto de distribución opera como servidor proxy de KSN
Alternar entre la ayuda en línea y la ayuda sin conexión
Exportación de eventos a sistemas SIEM
Configurar la exportación de eventos a sistemas SIEM
Antes de comenzar
Acerca de los eventos en Kaspersky Security Center
Acerca de la exportación de eventos
Acerca de la configuración de la exportación de eventos en un sistema SIEM
Marcar los eventos que se exportarán a un sistema SIEM en formato Syslog
Marcar eventos de una aplicación de Kaspersky para exportarlos en formato Syslog
Marcar eventos generales para que se los exporte en formato Syslog
Acerca de la exportación de eventos en formato Syslog
Acerca de la exportación de eventos en formato CEF o LEEF
Configurar Kaspersky Security Center para exportar eventos a un sistema SIEM
Exportación de eventos directamente desde la base de datos
Ejecutar una consulta SQL con la utilidad klsql2
Ejemplo de una consulta de SQL usando la utilidad klsql2
Visualización del nombre de la base de datos de Kaspersky Security Center
Ver los resultados de la exportación
Usar SNMP para enviar estadísticas a aplicaciones de terceros
Configuración del servicio SNMP para usar con Kaspersky Security Center
Agentes SNMP e identificadores de objetos
Obtener un nombre de contador de serie a partir de un identificador de objeto
Valores de identificadores de objetos para SNMP
Resolución de problemas
Trabajo en un entorno de nube

Acerca del trabajo en un entorno de nube
Escenario: Despliegue en un entorno de nube
Requisitos previos para desplegar Kaspersky Security Center en un entorno de nube
Requisitos de hardware para el Servidor de administración en un entorno de nube
Opciones de licencia en un entorno de nube
Opciones de base de datos para trabajar en un entorno de nube
Trabajar en el entorno de nube de Amazon Web Services
- Acerca del trabajo con el entorno de nube de Amazon Web Services
- Creación de funciones de IAM y cuentas de usuario de IAM para instancias de Amazon EC2
  - Comprobar que el Servidor de administración de Kaspersky Security Center tenga los permisos para trabajar con AWS
  - Crear una función de IAM para el Servidor de administración
  - Creación de una cuenta de usuario de IAM para trabajar con Kaspersky Security Center
  - Creación de una función de IAM para la instalación de aplicaciones en instancias de Amazon EC2
- Trabajar con Amazon RDS
  - Creación de una instancia de RDS de Amazon
  - Creación de un grupo de opciones para la instancia de RDS de Amazon
  - Modificación del grupo de opciones
  - Modificación de permisos para la función de IAM para la instancia de base de datos de Amazon RDS
  - Preparación del bucket de Amazon S3 para la base de datos
  - Migrar la base de datos a Amazonas RDS

Trabajar en el entorno de nube de Microsoft Azure
- Acerca del uso de Microsoft Azure
- Creación de una suscripción, un id. de aplicación y una contraseña
- Asignación de una función al id. de la aplicación en Azure
- Despliegue del Servidor de administración en Microsoft Azure y selección de la base de datos
- Trabajar con Azure SQL
  - Creación de la cuenta de almacenamiento de Azure
  - Creación de base de datos de SQL Azure y SQL Server
  - Migrar la base de datos a Azure SQL

Trabajar con Google Cloud
- Creación de correo electrónico de cliente, ID de proyecto y clave privada
- Trabajar con Google Cloud SQL para la instancia MySQL

Requisitos previos para dispositivos cliente en un entorno de nube necesarios para trabajar con Kaspersky Security Center
Creación de los paquetes de instalación necesarios para configurar el entorno de nube
Configuración del entorno de nube
- Acerca del asistente de configuración del entorno de nube
- Paso 1. Selección del método de activación de la aplicación
- Paso 2. Selección del entorno de nube
- Paso 3. Autorización en el entorno de nube
- Paso 4. Configuración de la sincronización con Cloud y elección de otras acciones
- Paso 5. Configuración de Kaspersky Security Network en el entorno de nube
- Paso 6. Configuración de notificaciones por correo electrónico en el entorno de nube
- Paso 7. Creación de una configuración inicial de la protección del entorno de nube
- Paso 8. Selección de la acción cuando el sistema operativo se debe reiniciar durante la instalación (para el entorno de nube)
- Paso 9. Recepción de actualizaciones por un Servidor de administración

Comprobación de la configuración
Grupo de dispositivos de nube
Sondeo de segmentos de red
Adición de conexiones para el sondeo de segmento de la nube
Eliminación de conexiones para el sondeo de segmento de la nube
Configuración de la programación de sondeos
Instalación de aplicaciones en dispositivos en un entorno de nube
Visualización de las propiedades de dispositivos de la nube
Sincronización con la nube
Despliegue de Kaspersky Security Center en Yandex.Cloud
Apéndices
Funciones avanzadas
Automatización del funcionamiento de Kaspersky Security Center. Utilidad klakaut
Herramientas personalizadas
Modo de clonación de disco del Agente de red
Preparación de un dispositivo de referencia con el Agente de red instalado para crear una imagen del sistema operativo
Configuración de la recepción de mensajes del Monitor de integridad de archivos
Mantenimiento del Servidor de administración
Acceso a los servidores DNS públicos
Ventana Método de notificación al usuario
Ventana Selección de dispositivos
Ventana Definir el nombre del nuevo objeto
Características de uso de la interfaz de administración
Árbol de consola
Cómo actualizar datos en el espacio de trabajo
Cómo navegar en el árbol de consola
Cómo abrir la ventana de propiedades de un objeto en el espacio de trabajo
Cómo seleccionar un grupo de objetos en el espacio de trabajo
Cómo cambiar el conjunto de columnas en el espacio de trabajo
Información de referencia
Comandos del menú contextual
Lista de dispositivos administrados. Descripción de las columnas
Estados de dispositivos, tareas y directivas
Icono de estado de archivo en la Consola de administración
Búsqueda y exportación de datos
Búsqueda de dispositivos
Configuración de la búsqueda de dispositivos
Uso de máscaras en variables de cadena
Uso de expresiones regulares en el campo de búsqueda
Exportación de listas desde cuadros de diálogo
Configuración de tareas
Configuración general de tareas
Ajustes de la tarea Descargar actualizaciones en el repositorio del Servidor de administración
Configuración de la tarea Descargar actualizaciones en los repositorios de los puntos de distribución
Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas
Configuración de la tarea Instalar actualizaciones requeridas y corregir vulnerabilidades
Lista global de subredes

Añadir subredes a la lista global de subredes
Ver y modificar las propiedades de subred en la lista global de subredes
Uso del Agente de red para Windows, Linux y macOS: comparación
Kaspersky Security Center Web Console
Diagrama de despliegue del Servidor de administración de Kaspersky Security Center y Kaspersky Security Center Web Console
Puertos usados por Kaspersky Security Center Web Console
Interfaz de Kaspersky Security Center Web Console
Anclar y desanclar secciones del menú principal
Escenario: Instalación y configuración inicial de Kaspersky Security Center Web Console
Instalación
Instalar Kaspersky Security Center (Instalación estándar)
Instalación de Kaspersky Security Center Web Console
Instalar Kaspersky Security Center Web Console conectado al Servidor de administración instalado en nodos del clúster de conmutación por error de Kaspersky
Actualización de Kaspersky Security Center Web Console
Certificados para trabajar con Kaspersky Security Center Web Console
Reemisión del certificado de Kaspersky Security Center Web Console
Reemplazo del certificado de Kaspersky Security Center Web Console
Especificación de certificados para Servidores de administración de confianza en Kaspersky Security Center Web Console
Conversión de un certificado PFX al formato PEM
Migración desde Kaspersky Security Center Windows
Migración a Kaspersky Security Center Cloud Console
Migrar a Kaspersky Next XDR Expert
Migración a Kaspersky Security Center Linux
Migrar a Kaspersky Security Center Linux con una copia de seguridad de los datos del Servidor de administración
Migración a Kaspersky Security Center Linux a través del Asistente de migración
Exportación de objetos de grupo desde Kaspersky Security Center Windows
Importar el archivo de exportación en Kaspersky Security Center Linux
Cambiar los dispositivos administrados para que estén bajo la administración de Kaspersky Security Center Linux
Iniciar y cerrar sesión en Kaspersky Security Center Web Console
Identity and Access Manager en Kaspersky Security Center Web Console
Acerca de Identity and Access Manager
Habilitación de Identity and Access Manager: escenario
Configuración de Identity and Access Manager en Kaspersky Security Center Web Console
Registro de la aplicación Kaspersky Industrial CyberSecurity for Networks en Kaspersky Security Center Web Console
Duración de los tokens y tiempo de espera de autorización para Identity and Access Manager
Descarga y distribución de certificados IAM
Deshabilitar Identity and Access Manager
Configurar la autenticación de dominio mediante los protocolos NTLM y Kerberos
Configuración del Servidor de administración
Configuración de la conexión de Kaspersky Security Center Web Console al Servidor de administración
Configurar el registro de eventos de conexiones del Servidor de administración
Configuración de las opciones de acceso a Internet para el Servidor de administración
Configuración del número máximo de eventos en el repositorio de eventos
Configuración de conexión de dispositivos con protección de UEFI

Creación de una jerarquía de servidores de administración: agregar un Servidor de administración secundario
Ver la lista de servidores de administración secundarios
Eliminar una jerarquía de servidores de administración
Mantenimiento del Servidor de administración
Configuración de la interfaz
Administración de servidores de administración virtuales
Crear un Servidor de administración virtual
Habilitación y deshabilitación de un Servidor de administración virtual
Asignar un administrador para un Servidor de administración virtual
Cambiar los dispositivos cliente de Servidor de administración
Eliminación de un Servidor de administración virtual
Habilitación de la protección de una cuenta desde la modificación no autorizada
Copia de seguridad y restauración de los datos del Servidor de administración
Creación de una tarea de copia de seguridad de datos
Mover el Servidor de administración a otro dispositivo
Comprobar la integridad de los módulos mediante las utilidades klscmodchk e Integrity_checker
Configuración inicial de Kaspersky Security Center Web Console
Asistente de inicio rápido (Kaspersky Security Center Web Console)
Paso 1. Especificar la configuración de la conexión a Internet
Paso 2. Descargando actualizaciones requeridas
Paso 3. Selección de los activos para asegurar
Paso 4. Seleccionar el cifrado en las soluciones
Paso 5. Configurar la instalación de los complementos para las aplicaciones administradas
Paso 6. Instalando los complementos seleccionados
Paso 7. Descarga de paquetes de distribución y creación de paquetes de instalación
Paso 8. Configurar Kaspersky Security Network
Paso 9. Selección del método de activación de la aplicación
Paso 10. Especificar la configuración de administración de las actualizaciones de terceros
Paso 11. Creación de una configuración básica de protección de la red
Paso 12. Configuración de notificaciones por correo electrónico
Paso 13. Realizar un sondeo de red
Paso 14. Cierre del asistente de inicio rápido
Conexión de dispositivos fuera de la oficina
Escenario: conexión de dispositivos fuera de la oficina mediante una puerta de enlace de conexión
Escenario: Conectar dispositivos fuera de la oficina mediante un Servidor de administración secundario en la DMZ
Acerca de la conexión de dispositivos fuera de la oficina
Conectar dispositivos de escritorio externos al Servidor de administración
Acerca de los perfiles de conexión para los usuarios fuera de la oficina
Creación de un perfil de conexión para usuarios fuera de la oficina
Acerca de cambiar el Agente de red a otros Servidores de administración
Creación de una regla de conmutación del Agente de red por ubicación de red
Asistente de despliegue de la protección
Paso 1. Iniciar el Asistente de despliegue de la protección
Paso 2. Seleccionar el paquete de instalación
Paso 3. Selección de un método para la distribución del archivo de clave o código de activación
Paso 4. Seleccionar la versión del Agente de red
Paso 5. Seleccionar los dispositivos

Paso 6. Configurar la tarea de instalación remota
Paso 7. Opciones de reinicio
Paso 8. Eliminar aplicaciones incompatibles antes de la instalación
Paso 9. Mover los dispositivos a Dispositivos administrados
Paso 10. Seleccionar cuentas con acceso a los dispositivos
Paso 11. Inicio de la instalación
Despliegue de aplicaciones de Kaspersky a través de Kaspersky Security Center Web Console
Escenario: despliegue de aplicaciones de Kaspersky a través de Kaspersky Security Center Web Console
La adquisición de complementos para aplicaciones de Kaspersky
Descargar y crear paquetes de instalación para aplicaciones de Kaspersky
Modificación del límite de datos para paquetes de instalación personalizados
Descargar paquetes de distribución para aplicaciones de Kaspersky
Verificar que Kaspersky Endpoint Security se haya desplegado correctamente
Creación de paquetes de instalación independientes
Ver la lista de paquetes de instalación independientes
Crear un paquete de instalación personalizado
Distribución de paquetes de instalación a servidores de administración secundarios
Instalar aplicaciones mediante la tarea de instalación remota
Instalación de una aplicación de forma remota
Instalar una aplicación mediante las directivas de grupo de Active Directory
Instalar aplicaciones en los Servidores de administración secundarios
Definir ajustes para instalaciones remotas en dispositivos Unix
Iniciar y detener aplicaciones de Kaspersky
Administración de dispositivos móviles
Reemplazo de aplicaciones de seguridad de terceros
Descubrimiento de dispositivos conectados a la red
Escenario: Descubrir dispositivos conectados a la red
Descubrimiento de dispositivos
Sondeo de la red de Windows
Sondeo de intervalos IP
Agregar y modificar un intervalo IP
Sondeo con Zeroconf
Sondeo del controlador de dominio
Autenticación y conexión a un controlador de dominio
Configurar un controlador de dominio Samba
Configuración de reglas de retención para dispositivos no asignados
Inventario de equipos
Agregar información sobre los dispositivos nuevos
Configurar criterios usados para los dispositivos de empresa
Aplicaciones de Kaspersky: licencias y activación
Licencias de aplicaciones administradas
Agregar una clave de licencia al repositorio del Servidor de administración
Agregar una clave de licencia del Servidor de administración
Distribución de claves de licencia a dispositivos cliente
Distribución automática de una clave de licencia
Visualización de información sobre las claves de licencia en uso
Eliminar una clave de licencia del repositorio

Revocar la aceptación de un Contrato de licencia de usuario final
Renovación de licencias para aplicaciones de Kaspersky
Utilizar Kaspersky Marketplace para elegir soluciones empresariales de Kaspersky
Configurar la protección de la red
Procedimiento: Configurar la protección de la red
Acerca de la administración de la seguridad centrada en el dispositivo y centrada en el usuario
Configuración y propagación de directivas: enfoque centrado en el dispositivo
Configuración y propagación de directivas: enfoque centrado en el usuario
Ajustes de la directiva del Agente de red
Comparación de la configuración de la directiva del Agente de red por sistemas operativos
Habilitar y deshabilitar el modo de bajo consumo de recursos para el Agente de red
Configuración manual de la directiva de Kaspersky Endpoint Security
Configurar Kaspersky Security Network
Comprobar la lista de las redes protegidas por Firewall
Desactivar el análisis de los dispositivos de red
Excluir detalles de software de la memoria del Servidor de administración
Configurar el acceso a la interfaz de Kaspersky Endpoint Security para Windows en las estaciones de trabajo
Guardar eventos de directivas importantes en la base de datos del Servidor de administración
Configuración manual de la tarea de grupo para actualizar Kaspersky Endpoint Security
Concesión de acceso sin conexión al dispositivo externo bloqueado por Control de dispositivos
Eliminación de aplicaciones o actualizaciones de software de forma remota
Tareas
Acerca de las tareas
Acerca del alcance de las tareas
Crear una tarea
Iniciar una tarea manualmente
Ver la lista de tareas
Configuración general de tareas
Exportar una tarea
Importar una tarea
Iniciar el Asistente para cambiar contraseñas de tareas
Paso 1. Especificar credenciales
Paso 2. Seleccionar una acción para realizar
Paso 3. Ver los resultados
Crear la tarea Ejecución remota de scripts
Instalar aplicaciones en dispositivos a distancia con la tarea Ejecución remota de scripts
Configurar notificaciones y supervisar la tarea Ejecución remota de scripts
Preparar un archivo para la tarea Ejecución remota de scripts
Crear un paquete de instalación basado en un archivo de manifiesto
Administración de dispositivos cliente
Configuración de un dispositivo administrado
Creación de grupos de administración
Agregar dispositivos a un grupo de administración en forma manual
Mover dispositivos o clústeres a un grupo de administración en forma manual
Crear reglas de movimiento de dispositivos
Copiar reglas de movimiento de dispositivos
Condiciones para una regla de movimiento de dispositivos

Sobre clústeres y conjuntos de servidores
Propiedades de un clúster o conjunto de servidores
Ver y configurar las acciones para dispositivos inactivos
Acerca de los estados del dispositivo
Configurar cambios de estado para los dispositivos
Conexión remota al escritorio de un dispositivo cliente
Conectarse a un dispositivo a través de Windows Desktop Sharing
Selecciones de dispositivos
Ver la lista de dispositivos de una selección de dispositivos
Crear una selección de dispositivos
Configurar una selección de dispositivos
Exportar la lista de dispositivos de una selección de dispositivos
Eliminación de dispositivos de los grupos de administración en una selección
Etiquetas de dispositivo
Creación de una etiqueta de dispositivo
Cambiar el nombre de una etiqueta de dispositivo
Eliminar una etiqueta de dispositivo
Ver los dispositivos que tienen asignada una etiqueta
Ver las etiquetas asignadas a un dispositivo
Etiquetar un dispositivo manualmente
Quitarle una etiqueta a un dispositivo
Ver las reglas de etiquetado automático de dispositivos
Modificación de una regla para etiquetar dispositivos automáticamente
Creación de una regla para etiquetar dispositivos automáticamente
Ejecución de reglas para etiquetar dispositivos automáticamente
Eliminación de una regla para etiquetar dispositivos automáticamente
Administrar las etiquetas de los dispositivos con la utilidad klscflag
Directivas y perfiles de directivas
Acerca de las directivas y perfiles de directivas
Acerca del candado y el bloqueo de ajustes
Herencia en las directivas y los perfiles de directivas
Jerarquía de directivas
Perfiles de directivas en una jerarquía de directivas
Cómo se implementan los valores de configuración en un dispositivo administrado
Administración de directivas
Ver la lista de directivas
Crear una directiva
Modificar una directiva
Ajustes generales de una directiva
Habilitar y deshabilitar una opción de herencia en las directivas
Copiar una directiva
Mover una directiva
Exportación de una directiva
Importación de una directiva
Ver el gráfico de distribución de una directiva
Eliminar una directiva
Administración de perfiles de directivas

Ver los perfiles de una directiva
Cambiar la prioridad de un perfil de directiva
Crear un perfil de directiva
Modificar un perfil de directiva
Copiar un perfil de directiva
Crear una regla de activación para un perfil de directiva
Eliminar un perfil de directiva
Protección y cifrado de datos
Ver la lista de unidades cifradas
Ver la lista de eventos de cifrado
Crear y ver informes de cifrado
Brindar acceso a una unidad cifrada en modo sin conexión
Usuarios y roles de usuario
Acerca de los roles de usuario
Ver cuentas y sesiones de usuario
Configurar los derechos de acceso a las funciones de la aplicación. Control de acceso basado en roles
Derechos de acceso a las funciones de la aplicación
Roles de usuario predefinidos
Asignación de derechos de acceso a objetos específicos
Asignar derechos de acceso a usuarios y grupos de seguridad
Agregar una cuenta de un usuario interno
Crear un grupo de seguridad
Editar una cuenta de un usuario interno
Editar un grupo de seguridad
Asignación de un rol a un usuario o a un grupo de seguridad
Agregar cuentas de usuario a un grupo interno de seguridad
Designación de un usuario como propietario de un dispositivo
Configurar la verificación en dos pasos para todos los usuarios
Acerca de la verificación en dos pasos
Habilitación de la verificación en dos pasos para su cuenta (Web Console)
Habilitar la verificación en dos pasos para su cuenta (basada en MMC)
Habilitar la verificación en dos pasos obligatoria para todos los usuarios (Web Console)
Habilitar la verificación en dos pasos para todos los usuarios (basada en MMC)
Deshabilitar la verificación en dos pasos para una cuenta de usuario (Web Console)
Deshabilitar la verificación en dos pasos para una cuenta de usuario (basada en MMC)
Deshabilitar la verificación en dos pasos obligatoria para todos los usuarios (Web Console)
Deshabilitar la verificación en dos pasos obligatoria para todos los usuarios (basada en MMC)
Excluir cuentas de la verificación en dos pasos (Web Console)
Excluir cuentas de la verificación en dos pasos (basada en MMC)
Editar el nombre del emisor de un código de seguridad (Web Console)
Editar el nombre del emisor de un código de seguridad (basada en MMC)
Configurar la verificación en dos pasos para su cuenta (Web Console)
Configurar la verificación en dos pasos para su cuenta (basada en MMC)
Generar una nueva clave secreta
Prohibir a los nuevos usuarios configurar la verificación en dos pasos por sí mismos
Asignar a un usuario como propietario del dispositivo tras instalar el Agente de red
Eliminar un usuario o un grupo de seguridad

Cambiar la contraseña de una cuenta de usuario
Creación de roles de usuario
Editar un rol de usuario
Editar el alcance de un rol de usuario
Eliminar un rol de usuario
Asociación de perfiles de directivas con roles
Propagación de roles de usuario a Servidores de administración secundarios
Cambiar la contraseña de una cuenta
Revocar los derechos de administrador local
Administración de revisiones de objetos
Devolver un objeto a una revisión anterior
Agregar una descripción a una revisión
Ver y guardar una revisión de la directiva
Eliminación de objetos
Kaspersky Security Network (KSN)
Acerca de KSN
Configurar el acceso a KSN
Habilitar y deshabilitar el uso de KSN
Ver la Declaración de KSN aceptada
Aceptar una Declaración de KSN actualizada
Verificar si el punto de distribución opera como servidor proxy de KSN
Escenario de actualización de Kaspersky Security Center y aplicaciones de seguridad administradas
Actualización de las bases de datos y las aplicaciones de Kaspersky
Procedimiento: actualización regular de bases de datos y aplicaciones de Kaspersky
Acerca de la actualización de las bases de datos, los módulos de software y las aplicaciones de Kaspersky
Crear la Descarga de actualizaciones para la tarea del repositorio del Servidor de administración
Comprobar actualizaciones descargadas
Creación de la tarea Descargar actualizaciones en los repositorios de los puntos de distribución
Habilitación y deshabilitación de actualizaciones automáticas y parches para componentes de Kaspersky Security Center
Instalación automática de actualizaciones para Kaspersky Endpoint Security para Windows
Aprobar y rechazar actualizaciones de software
Actualización del Servidor de administración
Habilitación y deshabilitación del modelo de descarga de actualizaciones sin conexión
Actualizar las bases de datos y los módulos de software de Kaspersky en dispositivos sin conexión
Copia de seguridad y restauración de complementos web
Ajuste de puntos de distribución y puertas de enlace de conexión
Configuración estándar de puntos de distribución: oficina única
Configuración estándar de puntos de distribución: varias oficinas remotas pequeñas
Acerca de la asignación de puntos de distribución
Asignar puntos de distribución automáticamente
Designación manual de puntos de distribución
Modificar la lista de puntos de distribución para un grupo de administración
Sincronización forzada
Habilitación de un servidor push
Administración de aplicaciones de terceros en dispositivos cliente
Instalación de actualizaciones para software de terceros
Procedimiento: Actualización de software de terceros

Instalación de actualizaciones para software de terceros
Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas
Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas
Crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades
Agregar reglas de instalación de actualizaciones
Crear la tarea Instalar actualizaciones de Windows Update
Ver información sobre las actualizaciones disponibles para el software de terceros
Exportar la lista de actualizaciones de software disponibles a un archivo
Aprobar y rechazar actualizaciones de software de terceros
Creación de la tarea Realizar la sincronización con Windows Update
Actualización automática de aplicaciones de terceros
Reparación de vulnerabilidades en el software de terceros
Procedimiento: búsqueda y reparación de vulnerabilidades de software de terceros
Acerca de la búsqueda y reparación de vulnerabilidades de software
Reparación de vulnerabilidades en el software de terceros
Crear la tarea Reparar vulnerabilidades
Crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades
Agregar reglas de instalación de actualizaciones
Selección de soluciones de usuario para vulnerabilidades de software de terceros
Ver información sobre las vulnerabilidades de software detectadas en todos los dispositivos administrados
Ver información sobre las vulnerabilidades de software detectadas en un dispositivo administrado específico
Ver estadísticas de las vulnerabilidades presentes en los dispositivos administrados
Exportar la lista de vulnerabilidades de software a un archivo
Ignorar vulnerabilidades de software
Administración de las aplicaciones que se ejecutan en los dispositivos cliente
Uso de Control de aplicaciones para administrar archivos ejecutables
Modos y categorías de Control de aplicaciones
Obtención y visualización de una lista de archivos ejecutables almacenados en los dispositivos cliente
Crear una categoría de aplicaciones con contenido agregado manualmente
Crear una categoría de aplicaciones con archivos ejecutables de dispositivos específicos
Creación de una categoría de aplicaciones que incluya archivos ejecutables de una carpeta seleccionada
Visualización de la lista de categorías de aplicaciones
Agregar archivos ejecutables vinculados a eventos a una categoría de aplicaciones
Configurar Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows
Obtener y ver una lista de aplicaciones instaladas en los dispositivos cliente
Crear un paquete de instalación para una aplicación de terceros usando la base de datos de Kaspersky
Ver y modificar la configuración de un paquete de instalación de una aplicación de terceros de la base de datos de Kaspersky
Configurar el paquete de instalación de una aplicación de terceros incluida en la base de datos de Kaspersky
Etiquetas de aplicación
Creación de una etiqueta de aplicación
Cambiar el nombre de una etiqueta de aplicación
Asignación de etiquetas a una aplicación
Quitarle una etiqueta a una aplicación
Eliminación de una etiqueta de aplicación
Supervisión e informes
Procedimiento: Supervisión y generación de informes

Acerca de los tipos de funciones de supervisión y generación de informes
Panel y widgets
Uso del panel
Agregar widgets al panel
Ocultar un widget del panel
Mover un widget en el panel
Cambiar el aspecto o el tamaño de un widget
Cambiar la configuración de un widget
Acerca del modo solo panel
Configuración del modo solo panel
Informes
Utilización de informes
Crear una plantilla de informe
Ver y editar las propiedades de una plantilla de informe
Exportación de un informe a un archivo
Generar y ver un informe
Crear una tarea de entrega de informes
Eliminación de plantillas de informes
Eventos y selecciones de eventos
Acerca de los eventos de Kaspersky Security Center
Utilización de selecciones de eventos
Crear una selección de eventos
Editar una selección de eventos
Ver una lista de una selección de eventos
Exportar una selección de eventos
Importar una selección de eventos
Ver los detalles de un evento
Exportar eventos a un archivo
Acceder al historial de un objeto desde un evento
Eliminar eventos
Eliminación de selecciones de eventos
Configuración del plazo de almacenamiento para un evento
Eventos de los componentes de Kaspersky Security Center
Estructura de datos utilizada para describir los tipos de eventos
Eventos del Servidor de administración
Eventos del Servidor de administración: nivel Crítico
Eventos del Servidor de administración: nivel Error funcional
Eventos del Servidor de administración: nivel Advertencia
Eventos del Servidor de administración: nivel Información
Eventos del Agente de red
Eventos del Agente de red: nivel Error funcional
Eventos del Agente de red: nivel Advertencia
Eventos del Agente de red: nivel Información
Eventos del Servidor de MDM para iOS
Eventos de errores funcionales del Servidor de MDM para iOS
Eventos de advertencia del servidor de MDM para iOS
Eventos informativos del servidor de MDM para iOS

Bloquear eventos frecuentes
Acerca del bloqueo de eventos frecuentes
Administrar el bloqueo de eventos frecuentes
Eliminar el bloqueo de eventos frecuentes
Recepción de eventos de Kaspersky Security for Microsoft Exchange Servers
Notificaciones y estados de los dispositivos
Uso de notificaciones
Visualización de notificaciones en pantalla
Acerca de los estados del dispositivo
Configurar cambios de estado para los dispositivos
Configurar el envío de notificaciones
Notificaciones de eventos que se muestran al ejecutar un archivo ejecutable
Novedades de Kaspersky
Acerca de las novedades de Kaspersky
Especificar la configuración de los anuncios de Kaspersky
Dejar de recibir las novedades de Kaspersky
Ver información sobre la detección de amenazas
Cloud Discovery
Habilitar Cloud Discovery mediante el widget
Agregar el widget de Cloud Discovery al panel
Ver información sobre el uso de servicios en la nube
Nivel de riesgo de un servicio en la nube
Bloquear el acceso a servicios en la nube no deseados
Registro de actividad de Kaspersky Security Center Web Console
Integración entre Kaspersky Security Center y otras soluciones
Establecer una conexión en segundo plano
Exportación de eventos a sistemas SIEM
Configurar la exportación de eventos a sistemas SIEM
Antes de comenzar
Acerca de los eventos en Kaspersky Security Center
Acerca de la exportación de eventos
Acerca de la configuración de la exportación de eventos en un sistema SIEM
Marcar los eventos que se exportarán a un sistema SIEM en formato Syslog
Acerca del marcado de los eventos que se exportarán a un sistema SIEM en formato Syslog
Marcar eventos de una aplicación de Kaspersky para que se los exporte en formato Syslog
Marcar eventos generales para que se los exporte en formato Syslog
Acerca de la exportación de eventos en formato CEF o LEEF
Conversión de eventos al formato CEF o LEEF
Acerca de la exportación de eventos en formato Syslog
Configurar Kaspersky Security Center para exportar eventos a un sistema SIEM
Exportación de eventos directamente desde la base de datos
Ejecución de una consulta SQL mediante la utilidad klsql2
Ejemplo de una consulta de SQL usando la utilidad klsql2
Visualización del nombre de la base de datos de Kaspersky Security Center
Ver los resultados de la exportación
Cómo trabajar con Kaspersky Security Center Web Console en un entorno de nube
Configuración del entorno de nube en Kaspersky Security Center Web Console

Paso 1. Comprobar los complementos y paquetes de instalación necesarios
Paso 2. Obtención de licencias de la aplicación
Paso 3. Selección del entorno de nube y autorización
Paso 4. Sondeo del segmento, opciones de sincronización con la nube y otras acciones
Paso 5. Seleccionar una aplicación para crear una directiva y tareas
Paso 6. Configuración de Kaspersky Security Network para Kaspersky Security Center
Paso 7. Creación de una configuración de protección inicial
Sondeo de segmentos de red con Kaspersky Security Center Web Console
Adición de conexiones para el sondeo de segmento de la nube
Eliminar conexiones para el sondeo de segmentos de nube
Programación de sondeos a través de Kaspersky Security Center Web Console
Ver los resultados del sondeo de segmentos de nube en Kaspersky Security Center Web Console
Visualización de las propiedades de dispositivos de nube en Kaspersky Security Center Web Console
Sincronización con la nube: Configuración de la regla de movimiento
Instalación remota de aplicaciones en máquinas virtuales de Azure
Creación de copia de seguridad de los datos del Servidor de administración en un DBMS en la nube
Diagnóstico remoto de dispositivos cliente
Abrir la ventana de diagnóstico remoto
Habilitar y deshabilitar el seguimiento para las aplicaciones
Descargar los archivos de seguimiento de una aplicación
Eliminar archivos de seguimiento
Descargar la configuración de las aplicaciones
Descargar registros de eventos
Iniciar, detener o reiniciar la aplicación
Realizar un diagnóstico remoto del Agente de red de Kaspersky Security Center y descargar los resultados
Ejecutar una aplicación en un dispositivo cliente
Crear un archivo de volcado para una aplicación
Ejecución de diagnósticos remotos en un dispositivo cliente basado en Linux
Descarga y eliminación de archivos de Cuarentena y Copia de seguridad
Descarga de archivos de Cuarentena y Copia de seguridad
Cambiar el idioma de la interfaz de Kaspersky Security Center Web Console
Guía de referencia de API
Prácticas recomendadas para proveedores de servicios
Planificación de la distribución de Kaspersky Security Center
Suministro de acceso a Internet al Servidor de administración
Configuración estándar de Kaspersky Security Center
Acerca de los puntos de distribución
Jerarquía de Servidores de administración
Servidores de administración virtuales
Administración de dispositivos móviles con Kaspersky Endpoint Security para Android
Despliegue y configuración inicial
Recomendaciones sobre la instalación del Servidor de administración
Creación de cuentas para los servicios del Servidor de administración en un clúster de conmutación por error
Selección de un DBMS
Especificación de la dirección del Servidor de administración
Configuración de protección en la red de una organización cliente
Configuración manual de la directiva de Kaspersky Endpoint Security

Configuración de la directiva en la sección Protección avanzada contra amenazas
Configuración de la directiva en la sección Protección básica contra amenazas
Configuración de la directiva en la sección Configuración general
Configuración de la directiva en la sección Configuración de eventos
Configuración manual de la tarea de grupo para actualizar Kaspersky Endpoint Security
Instalación manual de la tarea de grupo para analizar un dispositivo con Kaspersky Endpoint Security
Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas
Configuración manual de la tarea de grupo para la instalación de actualizaciones y la reparación de vulnerabilidades
Creación de una estructura de grupos de administración y asignación de puntos de distribución
Configuración estándar de un cliente MSP: oficina única
Configuración estándar de un cliente MSP: varias pequeñas oficinas remotas
Jerarquía de directivas, usando perfiles de directivas
Jerarquía de directivas
Perfiles de directivas
Tareas
Reglas de movimiento de dispositivos
Categorización del software
Acerca de las aplicaciones multiinquilino
Copia de seguridad y restauración de la configuración del Servidor de administración
Un dispositivo con el Servidor de administración es inoperable
La configuración del Servidor de administración o la base de datos es corrupta
Despliegue del Agente de red y de la aplicación de seguridad
Despliegue inicial
Configuración de instaladores
Paquetes de instalación
Propiedades MSI y archivos de transformación
Despliegue con herramientas de terceros para la instalación remota de aplicaciones
Información general sobre las tareas de instalación remotas en Kaspersky Security Center
Despliegue mediante directivas de grupo de Microsoft Windows
Despliegue forzado con la tarea de instalación remota de Kaspersky Security Center
Ejecución de paquetes independientes creados por Kaspersky Security Center
Opciones para la instalación manual de aplicaciones
Instalación remota de aplicaciones en dispositivos en los que se encuentra instalado el Agente de red
Opciones para controlar el reinicio de los dispositivos en la tarea de instalación remota
Conveniencia de actualizar las bases de datos en el paquete de instalación de una aplicación antivirus
Eliminación de las aplicaciones de seguridad de terceros incompatibles
Eliminar el Agente de red protegido con contraseña desde el símbolo del sistema
Utilización de herramientas para la instalación remota de aplicaciones en Kaspersky Security Center para ejecutar archivos ejecutables relevantes en dispositivos administrados
Supervisión del despliegue
Configuración de instaladores
Información general
Instalación en modo silencioso (con un archivo de respuesta)
Instalación del Agente de red en modo silencioso (sin un archivo de respuesta)
Configuración de instalación parcial a través de setup.exe
Parámetros de instalación del Servidor de administración
Configuración de la instalación del Agente de red

Infraestructura virtual
Sugerencias sobre la reducción de la carga en máquinas virtuales
Compatibilidad con máquinas virtuales dinámicas
Soporte de copia de máquinas virtuales
Soporte de reversión del sistema de archivos para dispositivos con Agente de red
Acerca de los perfiles de conexión para los usuarios fuera de la oficina
Despliegue de la característica Administración de dispositivos móviles
Conexión de dispositivos KES al Servidor de administración
Conexión directa de dispositivos al Servidor de administración
Esquema para conectar dispositivos KES al Servidor en el que se usa la delegación restringida de Kerberos (KCD)
Usar Firebase Cloud Messaging
Integración con una infraestructura de claves públicas
Servidor web de Kaspersky Security Center
Otro trabajo de rutina
Controlar los semáforos y los eventos registrados en la Consola de Administración
Acceso remoto a dispositivos administrados
Uso de la opción "No desconectarse del Servidor de administración" para proporcionar conectividad continua entre un dispositivo administrado y el Servidor de administración
Acerca de la comprobación de la hora de conexión entre un dispositivo y el Servidor de administración
Acerca de la sincronización forzada
Sobre la tunelización
Guía de dimensionamiento
Acerca de esta Guía
Información sobre las limitaciones de Kaspersky Security Center
Evaluaciones para Servidores de administración
Evaluación de recursos del hardware para el Servidor de administración
Requisitos de hardware para DBMS y el Servidor de administración
Evaluación de espacio de la base de datos
Calcular el espacio necesario en disco (con y sin el uso de la función Administración de vulnerabilidades y parches)
Evaluación del número y configuración de Servidores de administración
Recomendaciones para conectar máquinas virtuales dinámicas a Kaspersky Security Center
Cálculos para puntos de distribución y puertas de enlace de conexión
Requisitos para un punto de distribución
Cálculo de la cantidad de puntos de distribución y su configuración
Evaluación del número de pasarelas de conexión
Registro de información sobre eventos para tareas y directivas
Consideraciones específicas y configuración óptima de ciertas tareas
Frecuencia de descubrimiento de dispositivos
Tarea de copia de seguridad de datos del Servidor de administración y tarea de mantenimiento del Servidor de administración
Tareas de grupo para actualizar Kaspersky Endpoint Security
Tarea de inventario
Detalles de margen de la carga de la red entre Servidor de administración y dispositivos protegidos
Consumo de tráfico en diferentes escenarios
Uso promedio de tráfico por 24 horas
Contacto con el Servicio de soporte técnico
Cómo obtener soporte técnico

Consultas mediante Kaspersky CompanyAccount al servicio de soporte técnico
Obtener archivos de volcado del Servidor de administración
Fuentes de información sobre la aplicación
Glosario
Actualización
Actualización de Kaspersky Security Center
Actualización disponible
Administración centralizada de aplicaciones
Administración directa de aplicaciones
Administrador de Kaspersky Security Center
Administrador del cliente
Administrador del proveedor de servicios
Agente de autenticación
Agente de red
Aplicación incompatible
Archivo de clave
Ataque MITM
Bases de datos antivirus
Brote de virus
Carpeta Copia de seguridad
Certificado compartido
Certificado del Servidor de administración
Clave activa
Clave de acceso de AWS IAM
Clave de licencia adicional (o de reserva)
Cliente del Servidor de administración (dispositivo cliente)
Cloud Discovery
Complemento de administración
Configuración de la tarea
Configuración de programa
Consola de administración
Consola de administración de AWS
Copia de seguridad de los datos del Servidor de administración
Derechos de administrador
Directiva
Dispositivo con protección de UEFI
Dispositivo KES
Dispositivo MDM con iOS
Dispositivos administrados
Dominio de difusión
Entorno de nube
Estación de trabajo del administrador
Estado de protección
Estado de protección de la red
Función de IAM
Gravedad de un evento
Grupo de administración

Grupo de aplicaciones con licencia

Guía para reforzar la seguridad

HTTPS

Identity and Access Management (IAM)

Imagen de máquina de Amazon (AMI)

Instalación forzada

Instalación local

Instalación manual

Instalación remota

Instancia de Amazon EC2

Interfaz de programación de aplicaciones de AWS (API de AWS)

JavaScript

Kaspersky Private Security Network (KPSN)

Kaspersky Security Center System Health Validator (SHV)

Kaspersky Security Network (KSN)

Nagent ligero (LWNGT)

Nivel de importancia del parche

Operador de Kaspersky Security Center

Paquete de instalación

Perfil de aprovisionamiento

Perfil de configuración

Perfil de MDM para iOS

Periodo de vigencia de la licencia

Propietario del dispositivo

Protección antivirus para redes

Proveedor de servicios de protección antivirus

Puerta de enlace de conexión

Punto de distribución

Repositorio de eventos

Restauración

Restauración de los datos del Servidor de administración

Servidor de administración

Servidor de administración doméstico

Servidor de administración virtual

Servidor de dispositivos móviles

Servidor de MDM para iOS

Servidor web de Kaspersky Security Center

Servidores de actualizaciones de Kaspersky

SSL

Subred de reconocimiento de ubicación de red (NLA)

Tarea

Tarea de grupo

Tarea local

Tarea para dispositivos específicos

Tienda de aplicaciones

Umbral de actividad viral

Usuario de IAM

Usuarios internos
Vulnerabilidad
Windows Server Update Services (WSUS)
Zona desmilitarizada (DMZ)
Información sobre código de terceros
Avisos de marcas registradas
Problemas conocidos

# Ayuda de Kaspersky Security Center 15.1

| | | | |
|---|---|---|---|
|  | **Novedades**<br>Descubra las novedades de la última versión de la aplicación. |  | **Configurar la protección de la red**<br>Administrar la seguridad de la organización. |
|  | **Requisitos de hardware y software**<br>Compruebe qué sistemas operativos y versiones de aplicaciones son compatibles. |  | **Aplicaciones de Kaspersky. Actualización de bases de datos y módulos de software**<br>Mantenga la fiabilidad del sistema de protección. |
|  | **Despliegue y configuración inicial**<br>Planifique el uso de los recursos, instale el Servidor de administración, instale el Agente de red y las aplicaciones de seguridad en los dispositivos cliente, y consolide los dispositivos en grupos de administración. |  | **Supervisión e informes**<br>Ver su infraestructura, estados de protección y estadísticas. Administre el acceso a los servicios en la nube con Cloud Discovery. |
|  | **Descubrimiento de dispositivos conectados a la red**<br>Descubra los dispositivos nuevos y existentes en la red de su organización. |  | **Reemplazo de aplicaciones de seguridad de terceros**<br>Aprende métodos para desinstalar aplicaciones incompatibles. |
|  | **Aplicaciones de Kaspersky. Despliegue centralizado**<br>Despliegue aplicaciones de Kaspersky. |  | **Ajuste de puntos de distribución y puertas de enlace de conexión**<br>Configure sus puntos de distribución. |
|  | **Actualización de Kaspersky Security Center desde una versión anterior**<br>Actualice Kaspersky Security Center 15.1 desde una versión anterior. |  | **Prácticas recomendadas para proveedores de servicios (Ayuda en línea únicamente)**<br>Conozca las recomendaciones para instalar, configurar y usar la aplicación, así como las formas de resolver problemas típicos en la operación de la aplicación. |
|  | **Aplicaciones de Kaspersky. Licencias y activación**<br>Active las aplicaciones de Kaspersky en unos pocos pasos. |  | **Guía de dimensionamiento (Ayuda en línea únicamente)**<br>Para obtener un rendimiento óptimo en diversas condiciones, tenga en cuenta la cantidad de dispositivos en red, la topología de la red y el conjunto de funciones de Kaspersky Security Center que necesita. |
|  | **Exportación de eventos a sistemas SIEM**<br>Configure la exportación de eventos a los sistemas SIEM para su análisis. |  | **Administración de vulnerabilidades y parches**<br>Busque y corrija vulnerabilidades en las aplicaciones de otros desarrolladores. |
|  | **Trabajo en un entorno de nube**<br>Despliegue Kaspersky Security Center en un entorno de nube: Amazon Web Services™, Microsoft Azure™ y Google™ Cloud Platform. |  | **Preguntas frecuentes (solo en inglés)**<br>Encuentre instrucciones sobre cómo resolver problemas comunes. |
|  | **Guía de inicio rápido de Kaspersky Endpoint Security for Business**<br>Comience con Kaspersky Endpoint Security for Business: instale y configure esta solución. También puede ver la comparación de funciones de Kaspersky Security Center para elegir la forma más adecuada de administrar la seguridad de la red. | | |

# Novedades

## Kaspersky Security Center 15.1, actualización 2

Kaspersky Security Center 15.1, actualización 2 se centra en solucionar los problemas informados por los usuarios y el equipo de pruebas:

- Las tareas ahora se ejecutan correctamente para el alcance de los dispositivos administrados basados en Linux especificados al importar un archivo TXT.
- Ahora, cuando el instalador de una aplicación de Kaspersky se utiliza mediante una tarea de instalación remota creada en un Servidor de administración virtual, los paquetes de instalación se transmiten a los dispositivos administrados mediante el uso de herramientas del sistema operativo solo a través del punto de distribución administrado por ese Servidor de administración virtual.
- Se resolvió un problema por el cual un Servidor de administración secundario no podía volver a conectarse al Servidor de administración principal después de la rotación del certificado del Servidor secundario.
- Problemas resueltos que afectan las conexiones TLS.
- Se resolvió un problema que causaba varios errores de "conversión de tipo no válida" durante el inicio de sesión del usuario.
- Kaspersky Security Center ahora envía notificaciones de eventos por correo electrónico correctamente.
- Se solucionó un problema al agregar la carpeta *Actualizaciones* a la copia de seguridad al actualizar Kaspersky Security Center de la versión 14.2 a la versión 15.1.
- La fecha de vencimiento de la licencia de la aplicación de Kaspersky ahora se muestra correctamente en Kaspersky Security Center Web Console.
- Los comandos **Localizar el dispositivo móvil** y **Obtener historial de ubicaciones del dispositivo** ahora funcionan correctamente.
- Se solucionó un problema por el cual los paquetes de instalación con certificados para dispositivos móviles no se eliminaban automáticamente 1 hora después de la descarga o 24 horas después de permanecer sin usar.
- El perfil de directiva activa activado por una etiqueta específica ahora se aplica correctamente a los dispositivos cuyas descripciones contienen esa etiqueta.
- Se solucionó un problema que causaba que aparecieran mensajes de error de las bases de datos de PostgreSQL en el registro de eventos.
- La exclusión de una cuenta de la verificación en dos pasos ahora funciona correctamente.
- Se solucionó un problema por el cual el cierre de sesión de Kaspersky Security Center Web Console no funcionaba correctamente al usar la autenticación de dominio con Identity and Access Manager habilitado.
- Ahora, al hacer una actualización de un complemento web de administración, al hacer clic en el vínculo con la versión del complemento requerida, se inicia la descarga.

- Problemas resueltos en los informes:
  - Cuando crea una tarea de entrega para los informes de amenazas y actualizaciones, y establece la programación de la tarea en **Mensual**, los informes se completan con los datos correctamente.
  - En la plantilla *Informe sobre el estado de los componentes de la aplicación*, los filtros por nombre de componente se aplican correctamente.
  - El *informe del despliegue de la protección* ahora se puede filtrar para mostrar solo los dispositivos en los que las aplicaciones de Kaspersky no están instaladas. Esto ayuda a visualizar la cantidad de dispositivos donde se instalarán las aplicaciones.
- El widget de **Cloud Discovery** se muestra correctamente, tenga o no el derecho **Ejecutar** en el área **Funciones generales: funcionalidad básica**.
- Rendimiento mejorado de los procedimientos almacenados y las operaciones de las bases de datos.
- Se solucionó un problema por el cual los certificados caducados vinculados a usuarios inexistentes provocaban que el proceso de renovación se detuviera para todos los usuarios.
- Problemas resueltos que afectan el manejo adecuado de certificados.
- Después de actualizar Kaspersky Security Center de la versión 14.2 a la 15.1, la descarga de un paquete de instalación independiente desde un Servidor de administración virtual secundario en la Consola de administración ahora funciona correctamente.
- En Kaspersky Security Center Web Console, cuando habilita el uso de Kaspersky Security Network (KSN) en la directiva de la aplicación de Kaspersky, la aceptación de la Declaración de KSN no está disponible para las siguientes aplicaciones: Kaspersky Endpoint Security for Linux versión 12.2 o anterior, Kaspersky Industrial CyberSecurity for Linux Nodes versión 1.5 o anterior, Kaspersky Security for Virtualization Light Agent versión 6.0 y 6.1, Kaspersky Embedded Systems Security for Linux versión 3.3 y Kaspersky Security for Windows Server versión 11.0.1.897.
- Se solucionó un problema por el cual no se aplicaba un perfil de directiva a los dispositivos basados en Linux incluidos en un grupo de dominio de Active Directory.
- Se solucionó un problema que ocurría durante los intentos de conexión de varios Servidores de administración secundarios de segundo nivel al Servidor de administración principal.

## Kaspersky Security Center 15.1

Kaspersky Security Center 15.1 presenta un número de mejoras y características nuevas.

- Cloud Discovery. Es una función nueva que le permite supervisar el intento de uso de los servicios en la nube en los dispositivos administrados con Windows y bloquear el acceso a los servicios en la nube que considere no deseados. Esta función solo está disponible en Kaspersky Security Center Web Console.
- Sondeo del controlador de dominio ahora le permite sondear un controlador de dominio Samba a través de un punto de distribución con Linux. Se llevaron a cabo otras mejoras para poder sondear dominios de gran tamaño.
- Diagnóstico remoto de dispositivos administrados con Linux.
- Inventario ampliado de hardware de dispositivos macOS. El Agente de red en un dispositivo macOS envía la dirección MAC y el número de serie del dispositivo al Servidor de administración.

- Ahora puede verificar la conexión con un sistema SIEM.
- La longitud máxima de la contraseña para un usuario interno aumentó a 256 caracteres.
- Al migrar de Kaspersky Security Center Windows a Kaspersky Security Center Linux, ahora puede cambiar los dispositivos administrados para que estén bajo la administración de Kaspersky Security Center Linux restaurando el certificado y la clave privada del Servidor de administración desde una copia de seguridad.
- Cuando ejecuta la herramienta Cleaner o la utilidad klmover para eliminar un agente de red protegido con contraseña, se le solicitará que ingrese la contraseña de desinstalación.
- Para cambiar de Kaspersky Security for Windows Server a Kaspersky Endpoint Security para Windows ya no es necesario reiniciar el dispositivo de destino.
- Se puede asignar un usuario como propietario del dispositivo durante o después de la instalación del Agente de red en un dispositivo cliente en Linux.
- Ahora puede recibir un informe sobre la instalación remota cuando instale software en los dispositivos administrados mediante scripts personalizados.
- Cuando ejecuta varios scripts personalizados en un dispositivo administrado, puede establecer la prioridad de cada script para definir el orden de ejecución. Los scripts se ejecutarán de mayor a menor prioridad.
- Auditoría de directivas ampliada. Ahora puede ver el contenido de una revisión de la directiva y guardarla en un archivo. Actualmente, estas funciones solo están disponibles para la directiva del Servidor de administración y la directiva del Agente de red.
- Mejoras en la experiencia del usuario, entre ellas:
  - Personalización del menú principal mediante el anclado de secciones de Kaspersky Security Center Web Console para brindar un acceso rápido desde la sección **Anclado**.
  - Trabajo optimizado con tablas. La vista predeterminada de cada tabla ahora contiene las columnas más usadas. Además, ahora puede seleccionar todos los elementos de la página actual o de toda la tabla, así como ordenar los elementos de toda la tabla.
  - Mejora en la configuración de la entrega de informes. Ahora puede especificar la programación de entrega del informe y hasta 20 direcciones de correo electrónico a las cuales enviar el informe.
- Puede revocar los derechos de administrador local de las cuentas en dispositivos administrados con Linux. Ello brinda una capa de control adicional sobre las cuentas de usuario. Los derechos de administrador local pueden revocarse, por ejemplo, una vez que finaliza un encargo puntual.
- Puede cambiar la contraseña de la cuenta local en dispositivos administrados con Linux, por ejemplo, cuando el usuario olvida la contraseña de la cuenta local o para llevar a cabo un cambio de contraseña programado.
- En la subsección **Administración de certificados de usuario**, puede especificar qué certificados raíz instalar. Estos certificados se pueden utilizar, por ejemplo, para verificar la autenticidad de sitios web o servidores web.
- El Informe de ataques de red ahora incluye la dirección MAC y el puerto del dispositivo atacante.
- Una nueva opción para obligar a un usuario interno a cambiar una contraseña en el próximo intento de inicio de sesión en Kaspersky Security Center Web Console.
- Ya no se comprueba la existencia de una licencia comercial cuando se exportan eventos a un sistema SIEM en formatos CEF o LEEF.

- Cuando migra de una aplicación de Kaspersky a otra y la aplicación actual está protegida con contraseña, puede especificar la contraseña de desinstalación en la tarea de instalación remota.

- Exchange ActiveSync ya no es compatible.

## Kaspersky Security Center 14.2

Kaspersky Security Center 14.2 presenta un número de mejoras y características nuevas.

- Se lanzó una nueva Guía de sistema de protección. Le recomendamos que lea detenidamente la guía y siga las recomendaciones de seguridad para configurar Kaspersky Security Center y su infraestructura de red.

  Además, instale la última actualización de Kaspersky Security Center. Esta actualización incluye funciones de protección de la infraestructura, como la verificación en dos pasos de las cuentas de usuario y otras mejoras.

- Ahora, se verifica automáticamente que haya acceso a los servidores de Kaspersky. Si los servidores DNS configurados en el sistema no permiten acceder a los servidores de Kaspersky, la aplicación utiliza los servidores DNS públicos.

- Ahora es posible configurar derechos de usuario en un Servidor de administración virtual en cualquier momento y con independencia del Servidor de administración principal. Además, se pueden asignar a los usuarios de un Servidor principal los derechos necesarios para administrar un Servidor virtual.

- Kaspersky Security Center ahora permite utilizar los siguientes DBMS:

  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro 13.x (todas las ediciones)
  - Postgres Pro 14.x (todas las ediciones)
  - MariaDB 10.1, 10.4, 10.5

- Puede usar Kaspersky Security Center Web Console para exportar directivas y tareas a un archivo y luego importar esas directivas y tareas en Kaspersky Security Center Windows o Kaspersky Security Center Linux.

- La opción **No usar servidor proxy** ya no está disponible en las siguientes tareas:

  - *Descargar actualizaciones en el repositorio del Servidor de administración*
  - *Descargar actualizaciones en los repositorios de los puntos de distribución*

- Para proteger los dispositivos cliente en un entorno de nube, puede desplegar Kaspersky Endpoint Security para Windows en lugar de Kaspersky Security for Windows Server. Esta función ya está disponible después del lanzamiento de Kaspersky Endpoint Security 12.0 para Windows.

- El trabajo con las claves de cifrado ahora está limitado por los derechos de acceso al área funcional **Características generales**: **Administración de claves de cifrado**. Los usuarios de Kaspersky Security Center ahora pueden exportar claves de cifrado si tienen derechos de **Lectura** y pueden importar claves de cifrado si tienen derechos de **Escritura**.

# Kaspersky Security Center 14

Kaspersky Security Center 14 presenta un número de mejoras y características nuevas.

- La solución permite instalar actualizaciones y corregir vulnerabilidades de software de terceros en una red aislada (siempre que no se trate de software de Microsoft). Se denomina "red aislada" a aquella en la que el Servidor de administración y los dispositivos administrados no tienen acceso a Internet. Para corregir vulnerabilidades en este tipo de red, se necesita, en primer lugar, descargar las actualizaciones necesarias utilizando un Servidor de administración con acceso a Internet; una vez descargados, los parches se transmiten a los Servidores de administración aislados.

- Se han agregado perfiles de conexión para usuarios fuera de la oficina que utilizan dispositivos macOS. A través de estos perfiles, puede configurar reglas que hagan que, dependiendo de la ubicación de los dispositivos macOS, las copias del Agente de red instaladas en esos equipos se conecten a un mismo Servidor de administración o a servidores de administración diferentes.

- El Agente de red ahora se puede instalar en dispositivos con Microsoft Windows 10 IoT Enterprise.

- Puede aplicar un filtro en el **Informe de amenazas** para que, en la lista de amenazas, se muestren únicamente las amenazas detectadas por Cloud Sandbox.

- Kaspersky Security Center ahora admite Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 como aplicación administrada.

Kaspersky Security Center Web Console tiene varias funciones nuevas y mejoras:

- Puede configurar el modo Solo Panel para aquellos empleados que, sin ser responsables por la administración de la red, desean ver información estadística sobre la protección de la red en Kaspersky Security Center. Esta información podría resultar de interés para un alto ejecutivo, por ejemplo. Un usuario para el que se habilitó el modo solo panel tiene acceso únicamente a un panel con un conjunto de widgets predefinido. La persona puede monitorear las estadísticas que brinda cada widget (por ejemplo, el estado de protección de los dispositivos administrados, la cantidad de amenazas detectadas en tiempo reciente o la lista de amenazas más frecuentes en la red).

- Kaspersky Security Center Web Console ahora permite usar Kaspersky Security for iOS como aplicación de seguridad.

- En las propiedades de las tareas, ahora puede indicar si las tareas se aplicarán o no a los subgrupos y servidores de administración secundarios (incluidos los servidores de administración virtuales).

- Kaspersky Security Center ahora admite Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 como aplicación administrada.

## Kaspersky Security Center 13.2

Kaspersky Security Center 13.2 presenta un número de mejoras y características nuevas.

- Ahora puede instalar el Servidor de administración, la Consola de administración, Kaspersky Security Center 13.2 Web Console y el Agente de red en los siguientes sistemas operativos nuevos (consulte los requisitos de software para obtener más información):
  - Microsoft Windows 11.
  - Microsoft Windows 10 21H2 (actualización de octubre de 2021).
  - Windows Server 2022.
- Puede usar MySQL 8.0 como la base de datos.
- Puede desplegar Kaspersky Security Center en un clúster de conmutación por error de Kaspersky Security Center para proporcionar alta disponibilidad de Kaspersky Security Center.
- Kaspersky Security Center ahora funciona con direcciones IPv6 y direcciones IPv4. El Servidor de administración puede sondear las redes que tienen dispositivos con direcciones IPv6.

Kaspersky Security Center 13.2 Web Console tiene varias funciones nuevas y mejoras:

- Ahora puede administrar los dispositivos móviles con Android a través de Kaspersky Security Center 13.2 Web Console.
- Kaspersky Marketplace está disponible como una nueva sección del menú: puede buscar una aplicación de Kaspersky a través de Kaspersky Security Center 13.2 Web Console.
- Kaspersky Security Center ahora admite las siguientes aplicaciones de Kaspersky:
  - Kaspersky Endpoint Detection and Response Optimum 2.0
  - Kaspersky Sandbox 2.0
  - Kaspersky Industrial CyberSecurity for Networks 3.1

## Kaspersky Security Center 13.1

Kaspersky Security Center 13.1 presenta un número de mejoras y características nuevas.

- Se mejoró la integración con los sistemas SIEM. Ahora puede exportar eventos a los sistemas SIEM mediante el canal cifrado (TLS). La funcionalidad está disponible para Kaspersky Security Center Web Console y Consola de administración basada en MMC.
- Ya puede recibir parches para el Servidor de administración como un paquete de distribución, el cual puede usar para futuras actualizaciones de las versiones posteriores.
- Se agregó una nueva sección, **Alertas**, para Kaspersky Endpoint Detection and Response Optimum a Kaspersky Security Center 13.1 Web Console. También se agregaron nuevos widgets para trabajar con las amenazas que detecte Kaspersky Endpoint Detection and Response Optimum.

- En la Kaspersky Security Center 13.1 Web Console, ahora puede recibir notificaciones sobre licencias que caducan de las aplicaciones de Kaspersky.

- Se redujo el tiempo de respuesta de Kaspersky Security Center 13.1 Web Console.

## Kaspersky Security Center 13

Kaspersky Security Center 13 Web Console brinda las siguientes características nuevas:

- Verificación en dos pasos implementada. Puede habilitar la verificación en dos pasos para reducir el riesgo de acceso no autorizado a Kaspersky Security Center 13 Web Console.

- Se implementó la autenticación de dominio mediante los protocolos NTLM y Kerberos (inicio de sesión único). La función de inicio de sesión único le permite a un usuario de Windows habilitar la autenticación segura en Kaspersky Security Center 13 Web Console sin tener que volver a ingresar la contraseña en la red corporativa.

- Ahora puede configurar un complemento para que funcione con Kaspersky Managed Detection and Response. Puede utilizar esta integración para ver incidentes y administrar estaciones de trabajo.

- Ahora puede especificar la configuración de Kaspersky Security Center 13 Web Console en el asistente de instalación del Servidor de administración.

- Se muestran notificaciones sobre nuevas versiones de actualizaciones y parches. Puede instalar una actualización inmediatamente o más tarde, en cualquier momento. Ahora puede instalar parches para el Servidor de administración a través de Kaspersky Security Center 13 Web Console.

- Al trabajar con tablas, ahora puede especificar el orden y el ancho de las columnas, ordenar los datos y especificar el tamaño de la página.

- Ahora puede abrir cualquier informe al hacer clic en su nombre.

- Kaspersky Security Center 13 Web Console ahora está disponible en idioma coreano.

- Una nueva sección, Novedades de Kaspersky, está disponible en el menú **Supervisión e informes**. Esta sección lo mantiene informado al brindarle información relacionada con su versión de Kaspersky Security Center y las aplicaciones administradas instaladas en los dispositivos administrados. Kaspersky Security Center actualiza periódicamente la información de esta sección al eliminar anuncios obsoletos y agregar información nueva. Sin embargo, puede desactivar los anuncios de Kaspersky si lo desea.

- Se implementó una autenticación adicional después de cambiar la configuración de una cuenta de usuario. Puede habilitar la protección de una cuenta de usuario contra modificaciones no autorizadas. Si esta opción está habilitada, la modificación de la configuración de la cuenta de usuario requiere la autorización de un usuario con derechos de modificación.

Las siguientes funciones se agregan a Kaspersky Security Center 13:

- Verificación en dos pasos implementada. Puede habilitar la verificación en dos pasos para reducir el riesgo de acceso no autorizado a la Consola de administración. Si esta opción está habilitada, la modificación de la configuración de la cuenta de usuario requiere la autorización del usuario con derechos de modificación. Ya puede habilitar o deshabilitar la verificación en dos pasos para los dispositivos de KES.

- Puede enviar mensajes al Servidor de administración a través de HTTP. Ahora están disponibles una guía de referencia y una biblioteca de Python para trabajar con el OpenAPI del Servidor de administración.

- Puede emitir un certificado adicional para usar en los perfiles de MDM para iOS a fin de garantizar un cambio sin problemas de los dispositivos iOS administrados después de que caduque el certificado del servidor de MDM para iOS.

- La carpeta de aplicaciones multiinquilino ya no se muestra en la Consola de administración.

# Sobre Kaspersky Security Center

En esta sección, se brinda información sobre el objetivo, las características y los componentes principales de Kaspersky Security Center. Se describen, además, las maneras en que se puede adquirir Kaspersky Security Center.

La información que figura en Ayuda en línea puede diferir de la información proporcionada en los documentos enviados con la solicitud. En este caso, la Ayuda en línea se considera más actualizada. Puede pasar a la Ayuda en línea haciendo clic en los vínculos de la interfaz de la aplicación o haciendo clic en el vínculo Ayuda en línea de los documentos. La Ayuda en línea se puede actualizar sin notificación previa. Puede cambiar entre Ayuda en línea y Ayuda sin conexión de ser necesario.

Kaspersky Security Center está diseñado para ejecutar tareas de administración y mantenimiento básicas en la red de una organización de forma centralizada. La aplicación proporciona al administrador acceso a información detallada sobre el nivel de seguridad de la red de la organización; permite configurar todos los componentes de protección desarrollados usando las aplicaciones de Kaspersky.

Kaspersky Security Center es una aplicación pensada para administradores de redes corporativas y empleados responsables de la protección de dispositivos para una amplia variedad de organizaciones.

Si utiliza Kaspersky Security Center, puede realizar lo siguiente:

- Crear una jerarquía de los Servidores de administración para administrar la red de la organización, como también las redes en las oficinas remotas o en las organizaciones cliente.

  La *organización cliente* es una organización cuya protección antivirus está garantizada por un proveedor de servicios.

- Crear una jerarquía de grupos de administración para administrar una selección de dispositivos cliente como si fueran una sola entidad.

- Administrar un sistema de protección antivirus desarrollado sobre la base de las aplicaciones de Kaspersky.

- Crear imágenes de los sistemas operativos y desplegarlas en los dispositivos cliente a través de la red, como también realizar la instalación remota de las aplicaciones de Kaspersky y de otros proveedores de software.

- Administrar remotamente las aplicaciones desarrolladas por Kaspersky y otros proveedores e instaladas en dispositivos cliente. Actualizaciones de Instalar, encuentre y solucione vulnerabilidades.

- Llevar a cabo el despliegue centralizado de las claves de licencia de las aplicaciones Kaspersky en dispositivos cliente, supervise su utilización y renueve las licencias.

- Recibir estadísticas e informes sobre el funcionamiento de las aplicaciones y dispositivos.

- Recibir notificaciones sobre eventos críticos en la operación de aplicaciones de Kaspersky.

- Administrar dispositivos móviles.

- Administrar el cifrado de la información almacenada en unidades extraíbles y en los discos duros de los dispositivos, y el acceso de los usuarios a los datos cifrados.

- Realizar el inventario del hardware conectado a la red de la organización.
- Administrar de forma centralizada los archivos puestos en Cuarentena o Copia de seguridad por las aplicaciones de seguridad, y los archivos para los cuales se haya aplazado el procesamiento de parte de las aplicaciones de seguridad.

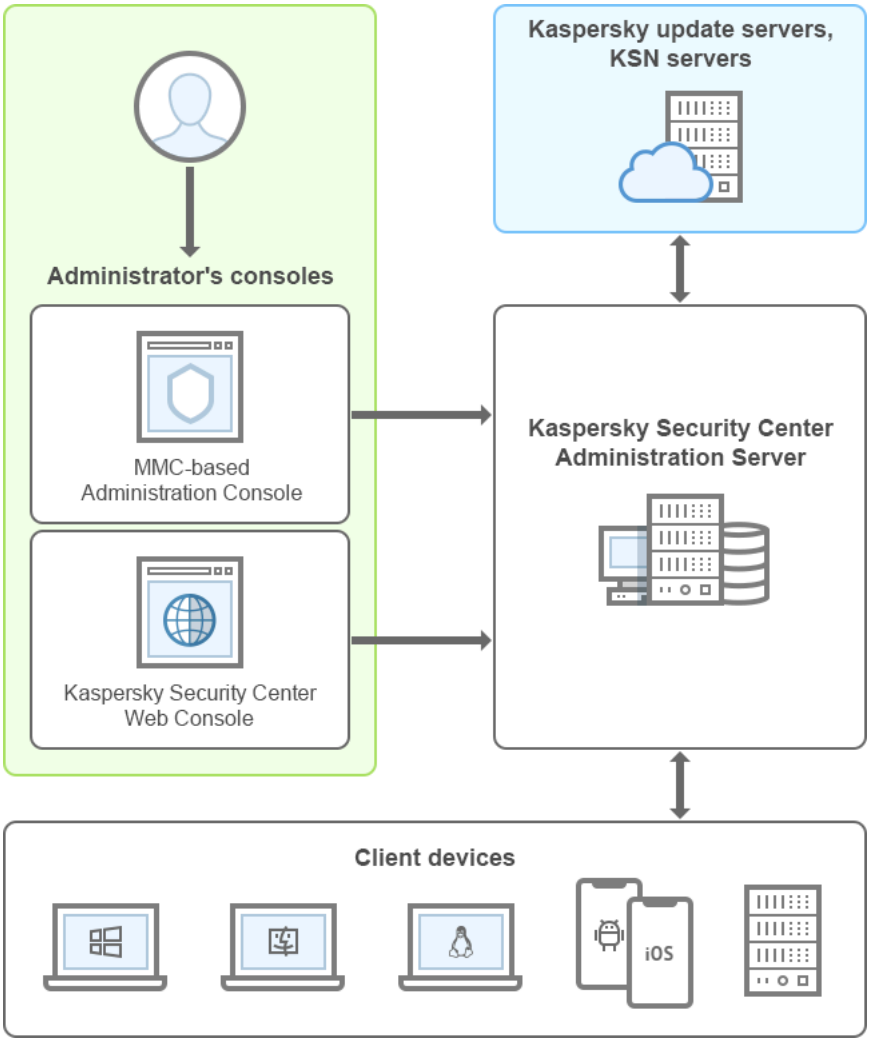
Puede comprar Kaspersky Security Center a través de Kaspersky (por ejemplo, en https://latam.kaspersky.com) o a través de empresas asociadas.

Si compra Kaspersky Security Center a través de Kaspersky, puede copiar la aplicación de nuestro sitio web. La información requerida para la activación de la aplicación se envía por correo electrónico después de procesar su pago.

Es posible que la funcionalidad de las actualizaciones (incluida la provisión de actualizaciones de firmas antivirus y actualizaciones de base de código) y la funcionalidad de KSN no estén disponibles en el software en los EE. UU.

# Arquitectura

Esta sección proporciona una descripción de los componentes de Kaspersky Security Center y su interacción.




Arquitectura de Kaspersky Security Center

Kaspersky Security Center comprende los siguientes componentes principales:

- *Consola de administración* (también conocida como *Consola*). La Consola de administración proporciona una interfaz de usuario a los servicios de administración del Servidor de administración y del Agente de red. La Consola de administración está implementada como un complemento de Microsoft Management Console (MMC). La Consola de administración permite la conexión remota al Servidor de administración a través de Internet.

- *Kaspersky Security Center Web Console*. Proporciona una interfaz web para crear y mantener el sistema de protección de la red de una organización cliente que es administrada por Kaspersky Security Center.

- *Servidor de administración de Kaspersky Security Center* (también denominado *Servidor*). Centraliza el almacenamiento de información sobre las aplicaciones instaladas en la red de la organización y sobre cómo administrarlas.

- *Servidores de actualizaciones de Kaspersky*. Servidores HTTP(S) de Kaspersky desde los que las aplicaciones de Kaspersky descargan actualizaciones para sus bases de datos y módulos de software.

- *Servidores de KSN*. Servidores que contienen una bases de datos de Kaspersky con información actualizada constantemente sobre la reputación de los archivos, recursos web y software. Kaspersky Security Network permite que las aplicaciones de Kaspersky respondan más rápidamente a las amenazas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de enfrentar falsos positivos.

- *Dispositivos cliente*. Dispositivos de la empresa cliente protegidos por Kaspersky Security Center. Cada dispositivo que debe protegerse debe tener instalada una de las aplicaciones de seguridad de Kaspersky.

# Requisitos de hardware y software

- Requisitos del Servidor de administración
- Requisitos de Web Console
- Requisitos de servidores móviles
- Requisitos de la Consola de administración
- Requisitos del Agente de red

## Requisitos del Servidor de administración

Requisitos de hardware mínimos:

- CPU con una frecuencia de funcionamiento de 1 GHz o más. Para sistemas operativos de 64 bits, la frecuencia mínima admisible es de 1.4 GHz.

- RAM: 4 GB.

- Espacio disponible en disco: 10 GB. Si va a utilizar la característica Administración de vulnerabilidades y parches, deberá tener al menos 100 GB de espacio disponible en disco.

Para despliegues en entornos de nube, los requisitos que se exigen para el Servidor de administración y el servidor de bases de datos son los mismos que se exigen para un Servidor de administración físico (los requisitos variarán en función de la cantidad de dispositivos que busque administrar).

Requisitos de software:

- Microsoft® Data Access Components (MDAC) 2.8
- Microsoft Windows® DAC 6.0
- Microsoft Windows Installer 4.5

Se admiten los siguientes sistemas operativos:

- Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core (64 bits)
- Windows Server 2016 Standard/Datacenter/Essentials/Server Core (opción de instalación) (LTSB) (64 bits)
- Windows Server 2019 Standard/Datacenter/Core (64 bits)
- Windows Server 2022 Standard/Datacenter/Core (64 bits)
- Windows Server 2025 Standard/Datacenter/Core (64 bits)
- Windows Storage Server 2019 (64 bits)

Se admiten las siguientes plataformas de virtualización:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- Microsoft Hyper-V Server 2019 (64 bits)
- Microsoft Hyper-V Server 2022 (64 bits)
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x

Se admiten los siguientes servidores de bases de datos (el servidor de bases de datos puede estar en un dispositivo diferente):

- Microsoft SQL Server 2016 (todas las ediciones) (64 bits)
- Microsoft SQL Server 2017 (todas las ediciones) en Windows/Linux (64 bits)
- Microsoft SQL Server 2019 (todas las ediciones) en Windows/Linux (64 bits) (requiere acciones adicionales)

- Microsoft SQL Server 2022 (todas las ediciones) en Windows/Linux (64 bits)
- MySQL 5.7 Community (32 bits o 64 bits)
- MySQL Standard Edition 8.0 (versión 8.0.20 y posterior) de 32 bits o 64 bits
- MySQL Enterprise Edition 8.0 (versión 8.0.20 y posterior) de 32 bits o 64 bits
- MariaDB 10.5 (compilación 10.5.27 y posteriores) (32 bits o 64 bits)
- MariaDB Galera Cluster 10.3 (32 bits o 64 bits) con motor de almacenamiento InnoDB
- PostgreSQL 13.x (64 bits)
- PostgreSQL 14.x (64 bits)
- PostgreSQL 15.x (64 bits)
- Postgres Pro 13.x Windows/Linux (64 bits)
- Postgres Pro 14.x Windows/Linux (64 bits)

Consulte el siguiente tema para obtener detalles y limitaciones: Selección de un DBMS.

Sistemas SIEM y otros sistemas de gestión de la información:

- HP (Micro Focus) ArcSight ESM 7.0
- IBM QRadar 7.3
- Splunk 7.1

# Requisitos de Web Console

## Servidor de Kaspersky Security Center Web Console

Requisitos de hardware mínimos:

- CPU: 4 núcleos, frecuencia de funcionamiento de 2.5 GHz
- RAM: 8 GB
- Espacio disponible en disco: 40 GB

Requisitos mínimos del certificado del Servidor de administración:

- Algoritmo de firma de certificado SHA-2
- Longitud mínima de la clave: 2048

Si necesita volver a emitir el certificado, consulte la Base

https://support.kaspersky.com/ksc/15.1/troubleshooting/other/15964#block8

de conocimientos de Kaspersky Security Center.

Sistemas operativos compatibles con Kaspersky Security Center Web Console

| | |
|---|---|
| Sistemas operativos. Microsoft Windows (solo versiones de 64 bits) | Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials (64 bits)<br>Windows Server 2016 Standard/Datacenter/Essentials/Server Core (opción de instalación) (LTSB)<br>Windows Server 2019 Standard/Datacenter/Core<br>Windows Server 2022 Standard/Datacenter/Core<br>Windows Server 2025 Standard/Datacenter/Core<br>Windows Storage Server 2019 |
| Plataformas de virtualización | VMware vSphere 6.7<br>VMware vSphere 7.0<br>VMware vSphere 8.0<br>Citrix XenServer 7.1 LTSR<br>Citrix XenServer 8.x<br>Parallels Desktop 18<br>Oracle VM VirtualBox 7.x |

### Dispositivos cliente

Para un dispositivo cliente, el uso de Kaspersky Security Center Web Console solo requiere un navegador.

La resolución de pantalla mínimas es 1366x768 píxeles.

Los requisitos de hardware y software del dispositivo son los mismos que los del navegador utilizado con Kaspersky Security Center Web Console.

Navegadores:

- Google Chrome 128.0.6613.120 o versiones posteriores
- Microsoft Edge 128.0.2739.67 o versiones posteriores
- Safari 17.6 en macOS
- Navegador "Yandex" 24.7.3.1081 o versiones posteriores
- Versión de soporte extendido de Mozilla Firefox 115.14.0 o versiones posteriores

## Requisitos de servidores móviles

### Servidor de MDM para iOS

Requisitos de hardware:

- CPU con una frecuencia de funcionamiento de 1 GHz o más. Para sistemas operativos de 64 bits, la frecuencia mínima admisible es de 1.4 GHz
- RAM: 2 GB
- Espacio disponible en disco: 2 GB

Requisitos de software: Microsoft Windows (la versión de sistema operativo requerida es la que imponen los requisitos del Servidor de administración).

# Requisitos de la Consola de administración

Requisitos de hardware:

- CPU con una frecuencia de funcionamiento de 1 GHz o más. Para sistemas operativos de 64 bits, la frecuencia mínima admisible es de 1.4 GHz.
- RAM: 512 MB.
- Espacio disponible en disco: 1 GB.

Requisitos de software:

- Sistema operativo de Microsoft Windows (la versión compatible del sistema operativo viene determinada por los requisitos del Servidor de administración):
  - Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials (64 bits)
  - Windows Server 2016 Standard/Datacenter/Essentials (LTSB) (64 bits)
  - Windows Server 2019 Standard/Datacenter (64 bits)
  - Windows Server 2022 Standard/Datacenter (64 bits)
  - Windows Server 2025 Standard/Datacenter/Core (64 bits)
  - Windows Storage Server 2019 (64 bits)
- Microsoft Management Console 2.0
- Microsoft Windows Installer 4.5
- Microsoft Internet Explorer 11.0 en cualquiera de estos sistemas operativos:
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019
  - Microsoft Windows Storage Server 2019
- Microsoft Edge en Microsoft Windows Server 2022 Standard

# Requisitos del Agente de red

Requisitos de hardware mínimos:

- CPU con una frecuencia de funcionamiento de 1 GHz o más. Para sistemas operativos de 64 bits, la frecuencia mínima admisible es de 1.4 GHz.
- RAM: 512 MB.
- Espacio disponible en disco: 1 GB.

Requisito de software para dispositivos con Linux: debe estar instalado el intérprete del lenguaje Perl versión 5.10 o posterior.

| | |
|---|---|
| Sistemas operativos. Microsoft Windows | Windows Embedded POSReady 2009 con el Service Pack más reciente (32 bits)<br>Windows Embedded 7 Standard con Service Pack 1 (32 bits o 64 bits)<br>Windows Embedded 8.1 Industry Pro (32 bits o 64 bits)<br>Windows 10 Enterprise 2015 LTSB (32 bits o 64 bits)<br>Windows 10 Enterprise 2016 LTSB (32 bits o 64 bits)<br>Windows 10 IoT Enterprise 2015 LTSB (32 bits o 64 bits)<br>Windows 10 IoT Enterprise 2016 LTSB (32 bits o 64 bits)<br>Windows 10 Enterprise 2019 LTSC (32 bits o 64 bits)<br>Windows 10 IoT Enterprise versión 1703 (32 bits o 64 bits)<br>Windows 10 IoT Enterprise versión 1709 (32 bits o 64 bits)<br>Windows 10 IoT Enterprise versión 1803 (32 bits o 64 bits)<br>Windows 10 IoT Enterprise versión 1809 (32 bits o 64 bits)<br>Windows 10 20H2 IoT Enterprise (32 bits o 64 bits)<br>Windows 10 21H2 IoT Enterprise (32 bits o 64 bits)<br>Windows 10 IoT Enterprise (32 bits o 64 bits)<br>Windows 10 IoT Enterprise versión 1909 (32 bits o 64 bits)<br>Windows 10 IoT Enterprise LTSC 2021 (32 bits o 64 bits)<br>Windows 10 IoT Enterprise versión 1607 (32 bits o 64 bits)<br>Windows 10 TH1 Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits)<br>Windows 10 TH2 Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits)<br>Windows 10 RS1 Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits)<br>Windows 10 RS2 Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits)<br>Windows 10 RS3 Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits)<br>Windows 10 RS4 Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits)<br>Windows 10 RS5 Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits)<br>Windows 10 RS6 Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits)<br>Windows 10 19H1 Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits)<br>Windows 10 19H2 Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits)<br>Windows 10 20H1 Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits)<br>Windows 10 20H2 Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits)<br>Windows 10 21H1 Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits)<br>Windows 10 21H2 Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits)<br>Windows 10 22H2 Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits)<br>Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education (64 bits)<br>Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education (64 bits)<br>Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education (64 bits)<br>Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education (64 bits)<br>Windows 8 Pro/Enterprise (32 bits o 64 bits)<br>Windows 8.1 Pro/Enterprise (32 bits o 64 bits)<br>Windows 7 Home/Pro/Enterprise/Ultimate con Service Pack 1 (32 bits o 64 bits)<br>Microsoft Windows XP Professional con Service Pack 2 32 bits / 64 bits (compatible solo con la versión 10.5.1781 del Agente de red, que puede solicitar al Soporte técnico)<br>Windows XP Professional con Service Pack 3 y versiones posteriores de 32 bits (compatible con la versión 14.0.0.20023 del Agente de red)<br>Windows XP Professional para sistemas integrados con Service Pack 3 de 32 bits (compatible con la versión 14.0.0.20023 del Agente de red)<br>Windows MultiPoint Server 2011 Standard/Premium (64 bits)<br>Windows Server 2003 SP1 de 32 bits / 64 bits (compatible solo con la versión 10.5.1781 del Agente de red)<br>Windows Server 2003 SP2 Standard/Enterprise 32 bits / 64 bits (compatible solo con la versión 10.5.1781 del Agente de red)<br>Windows Server 2003 R2 Standard/Enterprise con SP2 de 32 bits / 64 bits (compatible solo con la versión 10.5.1781 del Agente de red)<br>Windows Server 2008 Standard/Enterprise/Datacenter/Foundation con Service Pack 2 (32 bits o 64 bits)<br>Windows Server 2008 R2 Standard/Datacenter/Enterprise/Foundation con Service Pack 1 y versiones posteriores (64 bits)<br>Windows Server 2012 Standard/Datacenter/Essentials/Foundation/Server Core (64 bits) |

| | |
|---|---|
| | Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core (64 bits)<br>Windows Server 2016 Standard/Datacenter/Essentials/Server Core (opción de instalación) (LTSB) (64 bits)<br>Windows Server 2019 Standard/Datacenter/Core (64 bits)<br>Windows Server 2019 RS5 Standard/Essentials (64 bits)<br>Windows Server 2022 Standard/Datacenter/Core (64 bits)<br>Windows Server 2022 21H2 Standard/Datacenter (64 bits)<br>Windows Server 2025 Standard/Datacenter/Core (64 bits)<br>Windows Storage Server 2019 (64 bits) |
| Sistemas operativos. Linux | Debian GNU/Linux 10.x (Buster) (32 bits o 64 bits)<br>Debian GNU/Linux 11.x (Bullseye) (32 bits o 64 bits)<br>Debian GNU/Linux 12 (Bookworm) (32 bits o 64 bits)<br>Ubuntu Server 18.04 LTS (Bionic Beaver) (64 bits)<br>Ubuntu Server 20.04 LTS (Focal Fossa) (64 bits)<br>Ubuntu Server 22.04 LTS (Jammy Jellyfish) (64 bits)<br>Ubuntu Server 22.04 LTS ARM (64 bits)<br>Ubuntu Server 24.04 LTS (Noble Numbat) (64 bits)<br>CentOS 6.7 y versiones posteriores (32 bits)<br>CentOS 6.x (hasta la versión 6.6) (32 bits o 64 bits)<br>CentOS 7.x (64 bits)<br>CentOS Stream 8 (64 bits)<br>CentOS Stream 9 (64 bits)<br>CentOS Stream 9 ARM (64 bits)<br>Red Hat Enterprise Linux Server 6.x (32 bits o 64 bits)<br>Red Hat Enterprise Linux Server 7.x (64 bits)<br>Red Hat Enterprise Linux Server 8.x (64 bits)<br>Red Hat Enterprise Linux Server 9.x (64 bits)<br>SUSE Linux Enterprise Server 12, todos los Service Pack (64 bits)<br>SUSE Linux Enterprise Server 15, todos los Service Pack (64 bits)<br>SUSE Linux Enterprise Server 15 (todos los Service Packs) ARM (64 bits)<br>openSUSE 15 (64 bits)<br>EulerOS 2.0 SP10 (64 bits)<br>EulerOS 2.0 SP10 ARM (64 bits)<br>Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.5) (64 bits)<br>Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.6) (64 bits)<br>Astra Linux Special Edition RUSB.10015-16 (versión 1) (actualización operativa 1.6) (64 bits)<br>Astra Linux Special Edition RUSB.10015-17 (actualización operativa 1.7.3) (64 bits)<br>Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.7) (64 bits)<br>Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.8) (64 bits)<br>Astra Linux Special Edition RUSB.10015-37 (actualización operativa 7.7) (64 bits)<br>Astra Linux Special Edition RUSB.10152-02 (actualización operativa 4.7) ARM (64 bits)<br>Astra Linux Common Edition (actualización operativa 2.12) (64 bits)<br>ALT Workstation 10.1 (64 bits)<br>ALT Server 10.1 (64 bits)<br>ALT Education 10.1 (64 bits)<br>ALT SP Server 10 (32 bits o 64 bits)<br>ALT SP Server 10 ARM (64 bits)<br>ALT SP Workstation 10 (32 bits o 64 bits)<br>ALT SP Workstation 10 ARM (64 bits)<br>ALT Server 10 (64 bits)<br>ALT Server 10 ARM (64 bits)<br>ALT Workstation 10 (32 bits o 64 bits)<br>ALT 8 SP Workstation (8.4) ARM (64 bits)<br>ALT 8 SP Server (8.4) ARM (64 bits)<br>ALT 8 SP Server (LKNV.11100-01) (32 bits o 64 bits)<br>ALT 8 SP Server (LKNV.11100-02) (32 bits o 64 bits)<br>ALT 8 SP Server (LKNV.11100-03) (32 bits o 64 bits) |

| | |
|---|---|
| | ALT 8 SP Workstation (LKNV.11100-01) (32 bits o 64 bits)<br>ALT 8 SP Workstation (LKNV.11100-02) (32 bits o 64 bits)<br>ALT 8 SP Workstation (LKNV.11100-03) (32 bits o 64 bits)<br>Mageia 4 (32 bits)<br>Oracle Linux 7 (64 bits)<br>Oracle Linux 8 (64 bits)<br>Oracle Linux 9 (64 bits)<br>Linux Mint 20.x (64 bits)<br>Linux Mint 21.1 y versiones posteriores (64 bits)<br>AlterOS 7.5 y versiones posteriores (64 bits)<br>GosLinux IC6/7.17 (64 bits)<br>GosLinux IC6/7.2 (64 bits)<br>SberOS 3.3.1 (64 bits)<br>Plataforma V SberLinux OS Server (SLO) 8.8 (64 bits)<br>Plataforma V SberLinux OS Server (SLO) 8.9.2 (64 bits)<br>RED OS 7.3 ARM (64 bits)<br>RED OS 7.3 Server (64 bits)<br>RED OS 7.3 Certified Edition (64 bits)<br>RED OS 8 Certified Edition (64 bits)<br>ROSA Enterprise Linux Server 7.9 (64 bits)<br>ROSA Enterprise Linux Desktop 7.9 (64 bits)<br>ROSA COBALT 7.9 (64 bits)<br>ROSA CHROME 12 (64 bits)<br>AlmaLinux 8 y versiones posteriores (64 bits)<br>AlmaLinux 9 y versiones posteriores (64 bits)<br>Rocky Linux 8 y versiones posteriores (64 bits)<br>Rocky Linux 9 y versiones posteriores (64 bits)<br>Atlant, compilación Alcyone, versión 2022.02 (64 bits)<br>Msvsphere 9.2 Server (64 bits)<br>Msvsphere 9.2 ARM (64 bits)<br>SynthesisM Server 8.6 (64 bits)<br>SynthesisM Client 8.6 (64 bits)<br>OSnova 2.10 (64 bits)<br>Kylin 10 (64 bits)<br>EMIAS 1.0 (64 bits)<br>Amazon Linux 2 (64 bits)<br>MosOS 15.4 Arbat (64 bits)<br>OS MES (Moscow Electronic School) (64 bits) |
| Sistemas operativos. macOS | Para obtener una lista de los sistemas operativos compatibles, consulte la Ayuda de Kaspersky Endpoint Security for Mac. |

El Agente de red es compatible con las arquitecturas Apple Silicon (M1) e Intel.

Se admiten las siguientes plataformas de virtualización:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x

- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- KVM (todos los sistemas operativos Linux compatibles con el Agente de red)

En dispositivos con Windows 10 versiones RS4 o RS5, puede que Kaspersky Security Center no detecte algunas vulnerabilidades en las carpetas en que esté activada la distinción entre mayúsculas y minúsculas.

Antes de instalar el Agente de red en dispositivos con Windows 7, Windows Server 2008 o Windows Server 2008 R2, asegúrese de haber instalado la actualización de seguridad KB3063858 para el sistema operativo de Windows (Actualización de seguridad para Windows 7 [KB3063858], Actualización de seguridad para Windows 7 para sistemas de 64 bits [KB3063858], Actualización de seguridad para Windows Server 2008 [KB3063858], Actualización de seguridad para Windows Server 2008 x64 Edition [KB3063858], Actualización de seguridad para Windows Server 2008 R2 x64 Edition [KB3063858]).

En Microsoft Windows XP, el Agente de red podría no realizar algunas operaciones correctamente.

Puede instalar o actualizar el Agente de red para Windows XP solo en Microsoft Windows XP. Las ediciones compatibles de Microsoft Windows XP y sus versiones correspondientes del Agente de red se enumeran en la lista de sistemas operativos compatibles. Puede descargar la versión que necesite del Agente de red para Microsoft Windows XP desde esta página.

Recomendamos instalar la misma versión del Agente de red que en Kaspersky Security Center.

Kaspersky Security Center es totalmente compatible con el Agente de red de la misma versión o posterior.

Network Agent para macOS se proporciona junto con la aplicación de seguridad Kaspersky para este sistema operativo.

# Aplicaciones y soluciones de Kaspersky compatibles

Puede usar Kaspersky Security Center para desplegar y administrar cualquier aplicación o solución de Kaspersky para la que hoy se ofrezca soporte. En la siguiente tabla, se enumeran las aplicaciones y soluciones de Kaspersky que son compatibles con la Consola de administración basada en MMC y con Kaspersky Security Center Web Console. Para conocer los números de versión de estas aplicaciones y soluciones, consulte la página web sobre el ciclo de vida del soporte para productos.

Lista de aplicaciones y soluciones de Kaspersky compatibles con Kaspersky Security Center

| Nombre de la aplicación o solución de Kaspersky | Compatible con la Consola de administración basada en MMC | Compatible con Kaspersky Security Center Web Console |
|---|---|---|
| **Para estaciones de trabajo** | | |
| Kaspersky Endpoint Security para Windows | ✓ | ✓ |

| Nombre de la aplicación o solución de Kaspersky | Compatible con la Consola de administración basada en MMC | Compatible con Kaspersky Security Center Web Console |
|---|---|---|
| Kaspersky Endpoint Security for Linux | ✓ | ✓ |
| Kaspersky Endpoint Security for Linux Elbrus Edition | ✓ | ✓ |
| Kaspersky Endpoint Security for Mac | ✓ | ✓ |
| Kaspersky Endpoint Agent | ✓ | ✓ |
| Kaspersky Embedded Systems Security para Windows | ✓ | ✓ |
| Kaspersky Embedded Systems Security para Linux | — | ✓ |
| **Para soluciones industriales** | | |
| Kaspersky Industrial CyberSecurity for Nodes | ✓ | ✓ |
| Kaspersky Industrial CyberSecurity for Linux Nodes | ✓ | ✓ |
| Kaspersky Industrial CyberSecurity for Networks (no se admite el despliegue centralizado) | ✓ | ✓ |
| **Para dispositivos móviles** | | |
| Kaspersky Endpoint Security para Android | ✓ | ✓ |
| Kaspersky Security para iOS | — | ✓ |
| **Para servidores de archivos** | | |
| Kaspersky Security for Windows Server | ✓ | ✓ |
| Kaspersky Endpoint Security para Windows | ✓ | ✓ |
| Kaspersky Endpoint Security for Linux | ✓ | ✓ |
| **Para entornos virtuales** | | |
| Kaspersky Security for Virtualization Light Agent | ✓ | ✓ |
| Kaspersky Security for Virtualization Agentless | ✓ | — |
| **Para servidores de correo y colaboración** | | |
| Kaspersky Security for Microsoft Exchange Servers | ✓ | — |
| **Para la detección de ataques selectivos** | | |
| Kaspersky Sandbox Server | — | ✓ |
| Kaspersky Endpoint Detection and Response Optimum | — | ✓ |
| Kaspersky Managed Detection and Response | — | ✓ |
| **Para dispositivos KasperskyOS** | | |
| Kaspersky IoT Secure Gateway | — | ✓ |
| Kaspersky Thin Client | — | ✓ |
| **Bases de datos de reputación** | | |
| Kaspersky Private Security Network | — | ✓ |

# Licencias y funciones de Kaspersky Security Center 15.1

Kaspersky Security Center requiere una licencia para algunas de sus funciones.

La siguiente tabla muestra las licencias que cubren cada función de Kaspersky Security Center.

Para habilitar las funciones de Kaspersky Security Center, es necesario activar el Servidor de administración agregando una clave de licencia para el Servidor de administración.

Debe agregar manualmente una clave de licencia para cada Servidor de administración.

Licencias y características de Kaspersky Security Center

| Funciones de Kaspersky Security Center | Administración de vulnerabilidades y parches de Kaspersky | Kaspersky Endpoint Security for Business Select | Kaspersky Endpoint Security for Business Advanced | Kaspersky Total Security for Business | Kaspersky Hybrid Cloud Security Standard | Kaspersky Hybrid Cloud Security Enterprise | Kaspersky EDR Optimum |
|---|---|---|---|---|---|---|---|
| Evaluación de vulnerabilidades | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Administración de parches | ✓ | – | ✓ | ✓ | – | ✓ | ✓ |
| Control de acceso basado en roles | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Instalación de sistemas operativos y aplicaciones | ✓ | – | ✓ | ✓ | – | ✓ | ✓ |
| Administración de dispositivos móviles (es decir, administración de los dispositivos iOS y Android de los usuarios) | ✓ | ✓ | ✓ | ✓ | – | – | ✓ |
| Configuración del entorno de nube para trabajar en entornos de nube como AWS, Microsoft Azure y Google Cloud | – | – | – | – | ✓ | ✓ | – |
| Exportación de eventos a sistemas SIEM: Syslog | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Exportación de eventos a sistemas SIEM (QRadar de IBM y ArcSight de Micro Focus) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

# Acerca de la compatibilidad de los componentes de Kaspersky Security Center

En la siguiente tabla, puede encontrar información sobre la compatibilidad de los componentes de Kaspersky Security Center.

| Componente | Compatible con |
|---|---|
| Servidor de administración de Kaspersky Security Center 15.1 | • Consola de administración de Kaspersky Security Center 15.1.<br>• Kaspersky Security Center 15.1 Web Console.<br>• Agente de red de Kaspersky Security Center de las siguientes versiones: 16, 15.4, 15.1, 15, 14.2, 14. |
| Kaspersky Security Center 15.1 Web Console | Servidor de administración de Kaspersky Security Center de las siguientes versiones: 15.1 y 14.2. |
| Servidor de administración principal de Kaspersky Security Center 15.1 | Servidores de administración secundarios:<br>• Kaspersky Security Center 14 Windows.<br>• Kaspersky Security Center 14.2 Windows.<br>• Kaspersky Security Center 15.1 Windows.<br>• Kaspersky Security Center 14.2 Linux.<br>• Kaspersky Security Center 15 Linux.<br>• Kaspersky Security Center 15.1 Linux. |
| Servidor de administración secundario de Kaspersky Security Center 15.1 | Servidores de administración principales:<br>• Kaspersky Security Center 14 Windows.<br>• Kaspersky Security Center 14.2 Windows.<br>• Kaspersky Security Center 15.1 Windows.<br>• Kaspersky Security Center 14.2 Linux.<br>• Kaspersky Security Center 15 Linux.<br>• Kaspersky Security Center 15.1 Linux. |

Le recomendamos que utilice la última versión del Servidor de administración de Kaspersky Security Center y de Kaspersky Security Center Web Console. De lo contrario, la funcionalidad de Kaspersky Security Center puede verse limitada. Puede instalar y actualizar el Servidor de administración de Kaspersky Security Center y Kaspersky Security Center Web Console de forma independiente. Si lo hace, debe asegurarse de que la versión de Kaspersky Security Center Web Console instalada sea compatible con la versión del Servidor de administración al que busque conectarse.

Si tiene la última versión de Kaspersky Security Center Web Console y la versión anterior de Kaspersky Security Center, y se produce un error durante la autenticación del dominio, el texto del error contendrá un mensaje predeterminado.

# Comparación de Kaspersky Security Center: basado en Windows frente a basado en Linux

Kaspersky proporciona Kaspersky Security Center como una solución local para dos plataformas: Windows y Linux. En la solución basada en Windows, instala el Servidor de administración en un dispositivo Windows y la solución basada en Linux tiene la versión del Servidor de administración que está diseñada para instalarse en un dispositivo Linux. La presente ayuda en línea contiene información sobre Kaspersky Security Center Windows. Para obtener información detallada sobre la solución basada en Linux, consulte la Ayuda en línea de Kaspersky Security Center Linux.

La siguiente tabla le permite comparar las características principales de Kaspersky Security Center como solución basada en Windows y como solución basada en Linux.

| Característica o propiedad | Kaspersky Security Center | |
|---|---|---|
| | Solución basada en Windows | Solución basada en Linux |
| **Servidor de administración** | | |
| Ubicación del sistema de administración de bases de datos (DBMS) | Local | Local<br>(Microsoft SQL no es compatible) |
| Sistema operativo para instalar el Servidor de administración en | Windows | Linux |
| Jerarquía de Servidores de administración | ✓ | ✓ |
| Compatibilidad con Servidores de administración virtuales | ✓ | ✓ |
| Transmisión de estadísticas del Servidor de administración a aplicaciones de terceros mediante SNMP | ✓ | Se implementará en 2026 |
| Servidor web para publicar paquetes de instalación y otros archivos | ✓ | ✓ |
| Instalación del Servidor de administración en un clúster de conmutación por error de Windows Server | ✓ | — |
| **Consola de administración** | | |
| Tipo de Consola de administración | Basada en MMC y basada en la web | Basado en la web |
| Sistema operativo donde instalar la consola de administración web | Windows o Linux | Linux |
| Inicio de sesión en la consola mediante la autenticación del dominio | ✓ | ✓<br>El inicio de sesión único no es compatible con las versiones 15.1 a 15.4 inclusive |
| **Administración de dispositivos cliente y grupos de administración** | | |
| Número máximo de dispositivos administrados (por servidor de administración) | 100000 | 50 000 (con PostgreSQL y Postgres Pro) |
| Sondeo de red | ✓ | ✓<br>A partir de la versión 16, se admiten los controladores de dominio FreeIPA y ALD Pro |
| Protección de dispositivos administrados: Windows, Linux y macOS | ✓ | ✓ |
| Protección de dispositivos móviles | ✓<br>Administración básica de dispositivos móviles | ✓<br>MDM y uso de la funcionalidad Kaspersky Secure Mobility Management (con la licencia) |
| Administración de la protección de máquinas virtuales | ✓ | ✓ |
| Protección de infraestructuras de nubes públicas | ✓ | — |
| Conexión remota al escritorio de un dispositivo cliente | ✓ | ✓<br>A partir de la versión 15.3 |
| Protección y cifrado de datos | ✓ | ✓<br>En dispositivos administrados basados en Windows con Kaspersky Endpoint Security para Windows o Kaspersky Endpoint Security for Mac instalados |
| Despliegue del clúster de conmutación por error de Kaspersky Security Center | ✓ | ✓ |
| Compatibilidad con clústeres y matrices de servidores en grupos de administración | ✓ | ✓ |
| Jerarquía de grupos de administración | ✓ | ✓ |

| Característica o propiedad | Kaspersky Security Center | |
|---|---|---|
| | Solución basada en Windows | Solución basada en Linux |
| Agregar una puerta de enlace de conexión ubicada en una DMZ como punto de distribución | ✓ (Consola de administración basada en MMC) | Se implementará en 2026 |
| **Trabajar con los usuarios** | | |
| Creación y gestión de cuentas de usuario | ✓ | ✓ |
| **Administrar aplicaciones de Kaspersky** | | |
| Directivas para aplicaciones | ✓ | ✓ |
| Tareas para aplicaciones de Kaspersky | ✓ | ✓ |
| Kaspersky Security Network | ✓ | ✓ |
| Proxy de KSN | ✓ | ✓ |
| Kaspersky Private Security Network | ✓ | ✓ |
| Implementación centralizada de claves de licencia para aplicaciones de Kaspersky | ✓ | ✓ |
| Diagnóstico remoto de dispositivos cliente | ✓ | ✓ |
| Actualización automática de aplicaciones de Kaspersky | ✓ | ✓ |
| Compatibilidad con el Control de anomalías adaptativo | ✓ | ✓ |
| Administración de la seguridad centrada en el dispositivo | ✓ | ✓ |
| Gestión de seguridad centrada en el usuario | ✓ | ✓ |
| **Administración de sistemas** | | |
| Despliegue de sistemas operativos en dispositivos cliente | ✓ | — |
| Administración de licencias de terceros | ✓ | — |
| Uso del Servidor de administración como servidor WSUS | ✓ | ✓ (solo el modo de búsqueda pasiva de Windows Update) |
| **Administración de aplicaciones de terceros en dispositivos cliente** | | |
| Instalar actualizaciones de software de terceros y reparar vulnerabilidades de software de terceros | ✓ | ✓ |
| **Supervisión, informes y auditoría** | | |
| Administración de revisiones de objetos | ✓ | ✓ |
| Comparación de las revisiones de una directiva | ✓ | Se implementará en 2026 |
| Visualización y trabajo con alertas detectadas por Kaspersky Endpoint Detection and Response Optimum | ✓ | ✓ |
| Notificaciones sobre eventos ocurridos en dispositivos administrados | ✓ | ✓ |
| Supervisión del estado de las directivas y el estado de las tareas | ✓ | ✓ |
| **Integraciones** | | |
| Integración con Kaspersky Managed Detection and Response | ✓ | ✓ |

| Característica o propiedad | Kaspersky Security Center | |
|---|---|---|
| | Solución basada en Windows | Solución basada en Linux |
| Integración con sistemas SIEM | ✓ | ✓ (solo a través de syslog) |
| Exportación de eventos usando los formatos CEF y LEEF | ✓ | Se implementará en 2026 |

# Acerca de Kaspersky Security Center Cloud Console

El uso de Kaspersky Security Center como una aplicación local significa que usted instala Kaspersky Security Center, incluido el Servidor de administración, en un dispositivo local y administra el sistema de seguridad de red a través de la Consola de administración basada en Microsoft Management Console (disponible solo en Kaspersky Security Center Windows) o de Kaspersky Security Center Web Console.

Sin embargo, puede usar Kaspersky Security Center como un servicio en la nube. En este caso, los expertos de Kaspersky instalan y mantienen Kaspersky Security Center para usted en el entorno de nube, y Kaspersky le proporciona acceso al Servidor de administración como un servicio. Para administrar el sistema de seguridad de su red, utilizará una Consola de administración basada en la nube, llamada Kaspersky Security Center Cloud Console. La interfaz de esta consola se asemeja a la de Kaspersky Security Center Web Console.

La interfaz y la documentación de Kaspersky Security Center Cloud Console están disponibles en los siguientes idiomas:

- Inglés
- Francés
- Alemán
- Italiano
- Japonés
- Portugués (Brasil)
- Ruso
- Chino simplificado
- Español
- Español (Latinoamérica)
- Chino tradicional

Puede obtener más información sobre Kaspersky Security Center Cloud Console y sus características en la documentación de Kaspersky Security Center Cloud Console y en la documentación de Kaspersky Endpoint Security for Business.

# Kaspersky Security Center 15.1

Esta sección proporciona información sobre el uso de Kaspersky Security Center 15.1.

La información que figura en Ayuda en línea puede diferir de la información proporcionada en los documentos enviados con la solicitud. En este caso, la Ayuda en línea se considera más actualizada. Puede pasar a la Ayuda en línea haciendo clic en los vínculos de la interfaz de la aplicación o haciendo clic en el vínculo Ayuda en línea de los documentos. La Ayuda en línea se puede actualizar sin notificación previa. Puede cambiar entre Ayuda en línea y Ayuda sin conexión de ser necesario.

# Conceptos básicos

Esta sección explica los conceptos básicos relacionados con Kaspersky Security Center.

## Servidor de administración

Los componentes de Kaspersky Security Center permiten la administración remota de las aplicaciones Kaspersky instaladas en dispositivos cliente.

Los dispositivos con el componente Servidor de administración instalado serán mencionados como *Servidores de administración* (también denominados *Servidores*). Los Servidores de administración deben estar protegidos, incluida la protección física, contra cualquier acceso no autorizado.

El Servidor de administración se instala en un dispositivo como un servicio con el siguiente conjunto de atributos:

- Con el nombre "Servidor de administración de Kaspersky Security Center".
- Configurado para iniciarse automáticamente junto con el sistema operativo.
- Con la cuenta **LocalSystem** o la cuenta de usuario seleccionada durante la instalación del Servidor de administración.

El Servidor de administración cumple las siguientes funciones:

- Almacena la estructura de los grupos de administración.
- Almacena información sobre la configuración de los dispositivos cliente.
- Organizar los repositorios para paquetes de distribución de aplicaciones.
- Instalar de manera remota aplicaciones en dispositivos cliente y eliminarlas.
- Permite actualizar las bases de datos y los módulos de software de las aplicaciones de Kaspersky.
- Permite administrar directivas y tareas en los dispositivos cliente.

- Almacenar información sobre eventos producidos en dispositivos cliente.
- Generación de informes sobre el funcionamiento de aplicaciones Kaspersky.
- Permite distribuir claves de licencia a los dispositivos cliente y puede almacenar información sobre estas claves.
- Puede reenviar notificaciones sobre el progreso de las tareas (por ejemplo, sobre la detección de virus en un dispositivo cliente).

### Asignación de nombres a los Servidores de administración en la interfaz de la aplicación

En la interfaz de la Consola de administración basada en MMC y Kaspersky Security Center Web Console, los Servidores de administración pueden tener los siguientes nombres:

- Nombre del dispositivo del Servidor de administración, por ejemplo: "*nombre_del_dispositivo*" o "Servidor de administración: *nombre_del_dispositivo*".
- Dirección IP del dispositivo del Servidor de administración, por ejemplo: "*Dirección IP*" o "Servidor de administración: *Dirección IP*".
- Los Servidores de administración secundarios y los Servidores de administración virtuales tienen nombres personalizados que usted especifica cuando conecta un Servidor de administración virtual o secundario al Servidor de administración principal.
- Si usa Kaspersky Security Center Web Console instalado en un dispositivo con Linux, la aplicación mostrará los nombres de los servidores de administración que haya marcado como confiables en el archivo de respuesta.

Puede conectarse al Servidor de administración a través de la Consola de administración o de Kaspersky Security Center Web Console.

## Jerarquía de Servidores de administración

Los Servidores de administración se pueden organizar en una jerarquía. Cada Servidor de administración puede tener varios Servidores de administración secundarios (denominados *Servidores secundarios*) en diferentes niveles de anidamiento de la jerarquía. El nivel de anidamiento para los Servidores secundarios no está restringido. Por tanto, los grupos de administración del Servidor de administración principal incluirán los dispositivos cliente de todos los Servidores de administración secundarios. De esta manera, secciones independientes y aisladas de redes pueden ser administradas por diferentes Servidores de administración que, a su vez, están administrados por el Servidor principal.

*Los Servidores de administración virtuales* son un caso particular de Servidores de administración secundarios.

La jerarquía de Servidores de administración se puede usar para realizar lo siguiente:

- Disminuir la carga en el Servidor de administración (en comparación con un único Servidor de administración instalado para toda la red).
- Disminuir el tráfico de intranet y simplificar el trabajo con las oficinas remotas. No es necesario establecer conexiones entre el Servidor de administración principal y todos los dispositivos de red, que pueden estar ubicados, por ejemplo, en diferentes regiones. Es suficiente instalar, en cada segmento de red, un Servidor de administración secundario, distribuir los dispositivos entre grupos de administración de Servidores secundarios y establecer conexiones entre los Servidores secundarios y el Servidor principal sobre canales de comunicación rápida.

- Distribuir las responsabilidades entre los administradores de seguridad antivirus. Todas las capacidades para la administración centralizada y el control de la seguridad antivirus en las redes corporativas permanecen disponibles.

- Facilitar el uso de Kaspersky Security Center para los proveedores de servicios. Los proveedores de servicios únicamente necesitan instalar Kaspersky Security Center y Kaspersky Security Center Web Console. Para administrar un gran número de dispositivos cliente de distintas organizaciones, los proveedores pueden agregar servidores de administración secundarios (los cuales pueden ser virtuales) a la jerarquía de servidores de administración.

Cada dispositivo incluido en la jerarquía de grupos de administración puede estar conectado a un único Servidor de administración. Deberá monitorear la conexión entre dispositivos y servidores de administración independientemente. Use la función para la búsqueda de dispositivos en los grupos de administración de diferentes Servidores en función de los atributos de red.

# Servidor de administración virtual

El Servidor de administración virtual (también llamado *Servidor virtual*.) es un componente de Kaspersky Security Center cuyo propósito es administrar la protección antivirus de la red de la organización cliente.

El Servidor de administración virtual es una clase particular de Servidor de administración secundario. En comparación con un Servidor de administración físico, los servidores de administración virtuales tienen las siguientes restricciones:

- El Servidor de administración virtual puede crearse solamente en un Servidor de administración principal.

- El Servidor de administración virtual usa la base de datos del Servidor de administración principal. Los servidores de administración virtuales no son compatibles con la tarea de copia de seguridad y restauración de datos ni con la tarea de búsqueda y descarga de actualizaciones.

- El Servidor virtual no admite la creación de Servidores de administración secundarios (incluidos Servidores virtuales).

Además, el Servidor de administración virtual está sujeto a las siguientes restricciones:

- En la ventana de propiedades de los servidor de administración virtuales, el número de secciones está restringido.

- Para instalar aplicaciones de Kaspersky de manera remota en dispositivos cliente administrados por un Servidor de administración virtual, es necesario que uno de esos dispositivos tenga instalado el Agente de red. Esto se necesita para garantizar la comunicación con el Servidor de administración virtual. Luego de la primera conexión con el Servidor de administración virtual, ese dispositivo se designa automáticamente como punto de distribución y, por lo tanto, funciona como puerta de enlace para la conexión entre los dispositivos cliente y el Servidor de administración virtual.

- Un Servidor virtual solo puede sondear la red utilizando puntos de distribución.

- Para reiniciar un Servidor virtual que funciona incorrectamente, Kaspersky Security Center reinicia el Servidor de administración principal y todos los Servidores de administración virtuales.
- A los usuarios creados en un Servidor virtual no se les puede asignar una función en el Servidor de administración.

El administrador de un Servidor de administración virtual tiene todos los privilegios en este Servidor virtual particular.

# Servidor de dispositivos móviles

Un *Servidor de dispositivos móviles* es un componente de Kaspersky Security Center que proporciona acceso a dispositivos móviles y permite administrarlos mediante la Consola de administración. El Servidor de dispositivos móviles recibe información acerca de dispositivos móviles y almacena sus perfiles.

Kaspersky Security Center incluye el Servidor de MDM para iOS como servidor de dispositivos móviles. Este Servidor de dispositivos móviles se usa para administrar los dispositivos móviles que admiten el servicio de Apple Push Notification (APN).

Los servidores de dispositivos móviles de Kaspersky Security Center permiten administrar los siguientes objetos:

- Un dispositivo móvil individual.
- Varios dispositivos móviles.
- Varios dispositivos móviles conectados simultáneamente a un clúster de servidores. Después de conectarse a un clúster de servidores, el servidor de dispositivos móviles instalado en este clúster aparece en la Consola de administración como un único servidor.

# Servidor web

El *Servidor web* de Kaspersky Security Center (en adelante también denominado *Servidor web*) es un componente de Kaspersky Security Center que se instala junto con el Servidor de administración. El Servidor web está diseñado para transmitir paquetes de instalación independientes, perfiles de MDM para iOS y archivos de una carpeta compartida a través de una red.

Al crear un paquete de instalación independiente, éste se publica automáticamente en el servidor web. En la lista de paquetes de instalación independiente creados se muestra un enlace para descargar el paquete independiente. De ser necesario, puede cancelar la publicación del paquete independiente o publicarlo nuevamente en el servidor web.

Cuando crea un perfil de MDM para iOS para el dispositivo móvil del usuario, también se publica automáticamente en el Servidor web. El perfil publicado se elimina automáticamente del Servidor web tan pronto como se instala correctamente en el dispositivo móvil del usuario.

La carpeta compartida se utiliza para el almacenamiento de información disponible para todos los usuarios cuyos dispositivos se administren a través del Servidor de administración. Si el usuario no posee un acceso directo a la carpeta compartida, puede obtener información sobre esa carpeta en el servidor web.

Para brindar a los usuarios información de la carpeta compartida por medio del Servidor web, el administrador debe crear una subcarpeta llamada "Pública" en la carpeta compartida y pegar la información relevante en ella.

La sintaxis del enlace de transferencia de información es la siguiente:

`https://<nombre del Servidor web>:<puerto HTTPS>/public/<objeto>`

donde:

- `<Web Server name>` es el nombre de Kaspersky Security Center Web Server.
- `<HTTPS port>` es un puerto HTTPS del servidor web que ha sido definido por el administrador. El puerto HTTPS se puede configurar en la sección **Servidor web** de la ventana de propiedades del Servidor de administración. El número de puerto predeterminado es 8061.
- `<object>` es la subcarpeta o archivo al que el usuario tiene acceso.

El administrador puede enviar el nuevo enlace al usuario de cualquier manera que le resulte conveniente (por ejemplo, por correo electrónico).

Mediante este enlace, el usuario puede descargar la información solicitada a un dispositivo local.

# Agente de red

La interacción entre el Servidor de administración y los dispositivos está a cargo del componente *Agente de red* de Kaspersky Security Center. El Agente de red debe instalarse en todos los dispositivos en los que se utiliza Kaspersky Security Center para administrar las aplicaciones de Kaspersky.

El Agente de red se instala en un dispositivo como un servicio con el siguiente conjunto de atributos:

- Su nombre es "Agente de red de Kaspersky Security Center".
- Configurado para iniciarse automáticamente junto con el sistema operativo.
- Se ejecuta utilizando la cuenta LocalSystem.

Un dispositivo que tiene el Agente de red instalado se denomina *dispositivo administrado* o *dispositivo*.

El Agente de red se puede instalar en dispositivos Windows, Linux y Mac. Puede obtener el componente de una de las siguientes fuentes:

- Paquete de instalación almacenado en el Servidor de administración (para usar esta fuente, el Servidor de administración debe estar instalado).
- Paquete de instalación publicado en los servidores web de Kaspersky.

No es necesario instalar el Agente de red en el dispositivo donde se instala el Servidor de administración, ya que la versión de servidor de del Agente de red se instala automáticamente junto con el Servidor de administración.

El nombre del proceso que inicia el Agente de red es *klnagent.exe*.

El Agente de red se encarga de sincronizar el dispositivo administrado con el Servidor de administración. Recomendamos que el intervalo de sincronización (también llamado *latido*) se fije en 15 minutos por cada 10 000 dispositivos administrados.

# Grupos de administración

Un *grupo de administración* (de ahora en adelante *grupo*) es un conjunto lógico de dispositivos administrados que se han combinado en función de un rasgo específico para que se los pueda administrar como una única unidad de Kaspersky Security Center.

Todos los dispositivos administrados que pertenecen a un grupo de administración están configurados para lo siguiente:

- Ejecutar aplicaciones con una configuración en común. La configuración puede definirse mediante directivas de grupo.
- Usar un modo común de funcionamiento de las aplicaciones, mediante la creación de tareas de grupo con parámetros específicos. Puede usar tareas de grupo para, por ejemplo, crear e instalar un paquete de instalación común, actualizar las bases de datos y los módulos de una aplicación, realizar análisis a pedido y activar la protección en tiempo real.

Un dispositivo administrado puede pertenecer a un solo grupo de administración.

Los grupos y los servidores de administración se pueden organizar en jerarquías sin límites de anidamiento. Cada nivel de una jerarquía puede incluir servidores de administración secundarios y virtuales, grupos y dispositivos administrados. Puede mover dispositivos de un grupo a otro sin trasladar esos equipos físicamente. Por ejemplo, si un empleado de su empresa pasa del departamento de Contabilidad al departamento de Desarrollo, puede mover el dispositivo que utiliza esa persona del grupo de administración Contadores al grupo de administración Desarrolladores. Al efectivizarse el traspaso, el dispositivo recibirá automáticamente la configuración que los desarrolladores requieren para sus aplicaciones.

# Dispositivo administrado

Un *dispositivo administrado* es un dispositivo con Windows, Linux o macOS donde se ha instalado el Agente de red, o un dispositivo móvil con una aplicación de seguridad de Kaspersky instalada. Puede administrar dichos dispositivos creando tareas y directivos para las aplicaciones instaladas en estos dispositivos. También puede recibir informes de dispositivos administrados.

Puede hacer que un dispositivo administrado que no sea móvil funcione como un punto de distribución y como una puerta de enlace de conexión.

Un dispositivo puede estar administrado por un solo Servidor de administración. Un Servidor de administración puede administrar hasta 100 000 dispositivos, incluidos los dispositivos móviles.

# Dispositivo no asignado

Un *dispositivo no asignado* es un dispositivo en la red que no se ha incluido en ningún grupo de administración. Puede realizar algunas acciones en los dispositivos no asignados, por ejemplo, moverlos a grupos de administración o instalar aplicaciones.

Cuando se detecta un nuevo dispositivo en su red, este dispositivo va al grupo de administración de **Dispositivos no asignados**. Puede configurar reglas para que los dispositivos se muevan automáticamente a otros grupos de administración una vez que se detecten los dispositivos.

# Estación de trabajo del administrador

La *estación de trabajo del administrador* es un dispositivo en el cual se instala la Consola de administración o que se usa para abrir Kaspersky Security Center Web Console. Los administradores pueden usar estos dispositivos para administrar en forma remota y centralizada las aplicaciones de Kaspersky instaladas en los dispositivos cliente.

Después de haber instalado la Consola de administración en su dispositivo, aparecerá el icono que se usa para iniciar la Consola. Búsquelo en **Inicio** →**Programas** → menú **Kaspersky Security Center**.

No hay restricciones sobre el número de equipos administrador. Desde cualquier estación de trabajo del administrador, puede administrar grupos de administración de varios Servidores de administración en la red, al mismo tiempo. Puede conectar la estación de trabajo del administrador a un Servidor de administración (ya sea físico o virtual) de cualquier nivel de jerarquía.

Puede incluir la estación de trabajo del administrador en un grupo de administración como dispositivo cliente.

Dentro de los grupos de administración de cualquier Servidor de administración, el mismo dispositivo puede actuar como un cliente del Servidor de administración, un Servidor de administración o una estación de trabajo del administrador.

# Complemento de administración

Para administrar las aplicaciones de Kaspersky a través de la Consola de administración, se utiliza un componente específico llamado *complemento de administración*. Cada aplicación de Kaspersky que se puede administrar a través de Kaspersky Security Center incluye un complemento de administración.

Mediante el complemento de administración de aplicaciones, es posible realizar las siguientes acciones en la Consola de administración:

- Crear y editar las directivas y configuración de la aplicación, además de la configuración de las tareas de la aplicación.
- Obtener información sobre las tareas de la aplicación, eventos que se producen en su funcionamiento, y también estadísticas de funcionamiento de la aplicación recibidas desde dispositivos cliente.

Puede descargar los complementos de administración desde la página web del Servicio de soporte técnico de Kaspersky.

# Complemento web de administración

Para administrar las aplicaciones de Kaspersky en forma remota a través de Kaspersky Security Center Web Console, se utiliza un componente especial, llamado *complemento web de administración*. En lo sucesivo, el término *complemento de administración* hará referencia a un complemento web de administración. Un complemento de administración es una interfaz entre Kaspersky Security Center Web Console y una aplicación específica de Kaspersky. El complemento de administración permite configurar tareas y directivas para esa aplicación.

Puede descargar los complementos web de administración desde el sitio web de Kaspersky.

Un complemento de administración hace lo siguiente:

- Brinda una interfaz para crear y editar tareas y ajustes para una aplicación
- Brinda una interfaz para crear y editar las directivas y los perfiles de directivas que se utilizan para configurar los dispositivos y las aplicaciones de Kaspersky en forma remota y centralizada
- Transmite los eventos generados por una aplicación
- Brinda las funciones que permiten a Kaspersky Security Center Web Console mostrar los datos de funcionamiento y los eventos de una aplicación, así como las estadísticas transmitidas por los dispositivos cliente

# Directivas

Una *directiva* es un conjunto de valores de configuración que se aplican a una aplicación de Kaspersky en un grupo de administración y sus subgrupos. Puede instalar varias aplicaciones de Kaspersky en los dispositivos de un grupo de administración. Con Kaspersky Security Center, puede crear una única directiva para cada aplicación de Kaspersky disponible en un grupo de administración. Una directiva tiene uno de los siguientes estados (consulte la tabla a continuación):

Estado de la directiva

| Estado | Descripción |
|---|---|
| Activa | La directiva que se encuentra vigente en un dispositivo. Solo puede haber una directiva activa para cada aplicación de Kaspersky en cada grupo de administración. Los dispositivos aplican los valores configurados en la directiva activa a la aplicación de Kaspersky. |
| Inactiva | Una directiva que no se encuentra vigente en un dispositivo. |
| Fuera de la oficina | Una directiva "fuera de la oficina" entra en vigor (es decir, se activa) cuando el dispositivo sale de la red corporativa. |

Las directivas funcionan de acuerdo con las siguientes reglas:

- Es posible configurar más de una directiva, con distintos valores, para una misma aplicación.
- Solo puede haber una directiva activa para la aplicación actual.
- Puede activar una directiva inactiva para responder a un evento específico. Por ejemplo, puede aplicar ajustes de protección antivirus más estrictos durante un brote de virus.
- Una directiva puede tener directivas secundarias.

En general, puede usar las directivas como preparativos para situaciones de emergencia, como un ataque de virus. Si sufriera un ataque a través de unidades USB, por ejemplo, podría activar una directiva que bloqueara el acceso a ese tipo de unidades. Al hacerlo, la directiva que se encontrara activa hasta ese momento se desactivaría automáticamente.

Para poder hacer frente a distintas situaciones sin tener que mantener un grupo de directivas que difieran entre sí en unos pocos valores de configuración, puede usar perfiles de directivas.

Un *perfil de directiva* es un subconjunto de valores de configuración que se agrupan bajo un nombre y reemplazan los valores de configuración de una directiva. Un perfil de directiva afecta la constitución de los ajustes vigentes de un dispositivo administrado. Los *ajustes vigentes* de un dispositivo son aquellos que se encuentran en vigor en el mismo en un momento dado como resultado de aplicar la directiva, el perfil de directiva y la configuración local de una aplicación.

Los perfiles de directivas funcionan de acuerdo con las siguientes reglas:

- Un perfil de directiva entra en vigor cuando se cumple una condición de activación específica.
- Los perfiles de directivas contienen valores de configuración que difieren de los especificados en la directiva.
- La activación de un perfil de directiva modifica los ajustes vigentes del dispositivo administrado.
- Una directiva puede tener un máximo de 100 perfiles de directiva.

# Perfiles de directivas

Puede que a veces necesite crear varias versiones de una misma directiva para diferentes grupos de administración. En ese caso, probablemente quiera tener la capacidad de modificar la configuración de esas directivas centralmente. Las versiones de la directiva podrían diferir en uno o dos valores de configuración únicamente. Suponga, por ejemplo, que todos los contadores de su empresa están sujetos a una misma directiva, pero existe una diferencia: los contadores sénior tienen permiso para usar unidades de almacenamiento extraíbles, mientras que los contadores junior lo tienen prohibido. En tal caso, no será práctico valerse únicamente de la jerarquía de grupos de administración para aplicar las directivas a los dispositivos.

Para evitar la creación de varias instancias de una sola directiva, Kaspersky Security Center permite crear *perfiles de directivas*. Los perfiles de directivas permiten que los dispositivos de un mismo grupo de administración operen con diferentes configuraciones de directiva.

Un perfil de directiva es un subconjunto nominado de los valores de configuración definidos en una directiva. Este subconjunto de valores, que se distribuye a los dispositivos de destino junto con la propia directiva, entra en vigor cuando se presenta una condición específica, llamada *condición de activación del perfil*. Un perfil contiene solamente los valores de configuración que difieren de los de la directiva "básica" que se encuentra activa en el dispositivo administrado. Cuando el perfil se activa, se modifican los valores de configuración que la directiva "básica" había impuesto inicialmente en el dispositivo. La configuración toma los valores especificados en el perfil.

# Tareas

Kaspersky Security Center administra las aplicaciones de seguridad de Kaspersky instaladas en los dispositivos mediante la creación y ejecución de *tareas*. Las tareas son el medio que se utiliza para instalar, iniciar y detener aplicaciones, analizar archivos, actualizar bases de datos y módulos de software y realizar otras acciones en las aplicaciones.

Las tareas para una aplicación específica solo se pueden crear si el complemento de administración para esa aplicación está instalado.

Una tarea se puede ejecutar en el Servidor de administración o en un dispositivo.

Las siguientes tareas se realizan en el Servidor de administración:

- Distribución automática de informes
- Descarga de actualizaciones en el repositorio del Servidor de administración
- Copia de seguridad de los datos del Servidor de administración
- Mantenimiento de la base de datos
- Sincronización con Windows Update
- Creación de un paquete de instalación basado en la imagen del SO de un dispositivo de referencia

Los siguientes tipos de tareas se ejecutan en los dispositivos:

- *Tareas locales*. Son tareas que se ejecutan en un dispositivo específico.

  Las tareas locales pueden ser modificadas por el administrador usando herramientas de la Consola de administración, o por el usuario de un dispositivo remoto (por ejemplo, a través de la interfaz de aplicaciones de seguridad). Si el administrador y el usuario del dispositivo administrado modifican una tarea local al mismo tiempo, los cambios realizados por el administrador se consideran prioritarios y son los que entran en vigor.

- *Tareas de grupo*. Son tareas que se ejecutan en todos los dispositivos de un grupo específico.

  A menos que se especifique lo contrario en las propiedades de la tarea, una tarea de grupo también afecta a todos los subgrupos del grupo seleccionado. Una tarea de grupo también afecta (opcionalmente) a los dispositivos que se han conectado a Servidores de administración secundarios y virtuales incluidos en el grupo o en cualquiera de sus subgrupos.

- Tareas globales. Son tareas que se ejecutan en un conjunto de dispositivos que pueden o no pertenecer a un grupo.

Para cada aplicación, puede crear cualquier número de tareas de grupo, tareas globales o tareas locales.

Puede copiar, importar, exportar y eliminar tareas, consultar el progreso de su ejecución y modificar su configuración.

Para que una tarea se inicie en un dispositivo, la aplicación para la que se la ha creado debe estar en ejecución.

Los resultados de las tareas se guardan en el registro de eventos de Microsoft Windows y en el registro de eventos de Kaspersky Security Center, tanto de forma centralizada en el Servidor de administración como localmente en cada dispositivo.

No incluya datos privados en la configuración de las tareas. Por ejemplo, evite especificar la contraseña del administrador del dominio.

# Alcance de la tarea

El *alcance de una tarea* es el conjunto de dispositivos en los que se realiza esa tarea. Los tipos de alcance son los siguientes:

- Para una *tarea local*, el alcance es el propio dispositivo.
- Para una *tarea del Servidor de administración*, el alcance es el Servidor de administración.
- Para una *tarea de grupo*, el alcance es la lista de dispositivos incluidos en el grupo.

Al crear una *tarea global*, puede usar los siguientes métodos para especificar su alcance:

- Especificar dispositivos puntuales manualmente.

  Para indicar la dirección de cada dispositivo, puede utilizar una dirección IP (o un intervalo IP), un nombre NetBIOS o un nombre DNS.

- Importar una lista de dispositivos de un archivo .TXT que contenga, en líneas separadas, la dirección de cada dispositivo que se quiera agregar.

  Si importa una lista almacenada en un archivo o crea una lista manualmente y elige identificar los dispositivos por nombre, tenga en cuenta que la lista únicamente podrá incluir dispositivos sobre los que ya haya información en la base de datos del Servidor de administración. Dicha información deberá haberse cargado durante la conexión o el descubrimiento de los dispositivos.

- Especificar una selección de dispositivos.

  El alcance de una tarea cambia con el tiempo, según cambia el conjunto de dispositivos incluidos en la selección. Puede generar una selección de dispositivos basada en los atributos de los dispositivos que quiera incluir (por ejemplo, el software instalado) o en las etiquetas asignadas a esos dispositivos. Una selección de dispositivos es la opción más flexible para especificar el alcance de una tarea.

  Las tareas para selecciones de dispositivos siempre son ejecutadas por el Servidor de administración en forma programada. Estas tareas no se pueden ejecutar en dispositivos que carecen de conexión con el Servidor de administración. Las tareas cuyo alcance se especifica mediante otros métodos se ejecutan directamente en los dispositivos y, por lo tanto, no dependen de la conexión del dispositivo al Servidor de administración.

  Las tareas para selecciones de dispositivos no se ejecutan según la hora local del dispositivo, sino según la hora local del Servidor de administración. Cuando el alcance se especifica por otros medios, la tarea se ejecuta según la hora local del dispositivo.

# Modo en que se relacionan las directivas y la configuración local de una aplicación

Puede usar directivas para que una aplicación opere con los mismos valores de configuración en todos los dispositivos de un grupo.

Si necesita redefinir los valores de configuración especificados por una directiva para ciertos dispositivos de un grupo, puede hacerlo modificando la configuración local de la aplicación. Tenga en cuenta que solo podrá modificar los valores de configuración que la directiva permita modificar, es decir, los de aquellos ajustes o parámetros que se encuentren desbloqueados.

El valor que una aplicación utiliza para un parámetro en un dispositivo cliente depende de si dicho parámetro está o no bloqueado (🔒) en la directiva:

- Cuando no está permitido modificar un parámetro, todos los dispositivos cliente utilizan el mismo valor (el que se ha fijado en la directiva).
- Cuando está permitido modificar un parámetro, en lugar del valor exigido por la directiva, la aplicación usa el valor definido localmente en el dispositivo cliente. Ello significa que el valor puede modificarse en la configuración local de la aplicación.

Así, cuando se ejecuta una tarea en un dispositivo cliente, la aplicación aplica valores configurados por dos vías diferentes:

- por medio de la configuración de la tarea y la configuración local de la aplicación, si la directiva no prohíbe los cambios en el parámetro correspondiente;
- por medio de la directiva de grupo, si la directiva prohíbe los cambios en el parámetro correspondiente.

La configuración local de una aplicación toma los valores definidos en una directiva la primera vez que se aplica esa directiva.

# Punto de distribución

Un *punto de distribución* (anteriormente conocido como agente de actualización) es un dispositivo con el Agente de red instalado que se utiliza para distribuir actualizaciones, instalar de forma remota las aplicaciones y recuperar la información relativa a los dispositivos en red. Los puntos de distribución aceleran la distribución de actualizaciones y liberan recursos en el Servidor de administración.

Las funciones y los casos de uso del Agente de red instalado en un dispositivo utilizado como punto de distribución varían según el sistema operativo.

Un punto de distribución puede realizar las siguientes funciones:

- Distribuir los archivos recibidos del Servidor de administración a los dispositivos cliente dentro del grupo (incluida la multidifusión a través de UDP).

  La lista de archivos que se pueden transferir mediante puntos de distribución incluye:

  - Actualizaciones de las bases de datos y módulos de software de Kaspersky
  - Actualizaciones para el software de terceros
  - Paquetes de instalación
  - Actualizaciones de Windows si utiliza el Servidor de Administración como servidor WSUS

  Las actualizaciones se pueden recibir desde el Servidor de administración o desde los servidores de actualización de Kaspersky. En el segundo caso, se debe crear una tarea de actualización para el punto de distribución. Los puntos de distribución con macOS no pueden descargar actualizaciones de los servidores de actualizaciones de Kaspersky.

  > Si hay uno o más dispositivos con macOS en el alcance de la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*, la tarea terminará con el estado *Error* aunque se complete sin errores en todos los dispositivos con Windows.

- Distribuir directivas y tareas de grupo mediante la multidifusión con UDP.

- Ejercer de puerta de enlace de conexión para el Servidor de administración para los dispositivos del grupo de administración.

  Cuando los dispositivos administrados de un grupo no se pueden conectar en forma directa con el Servidor de administración, el punto de distribución puede actuar como puerta de enlace para el grupo y facilitar la conexión con el Servidor de administración. Los dispositivos administrados se conectan a la puerta de enlace de conexión, y esta, a su vez, se conecta al Servidor de administración.

  Aun cuando existe un punto de distribución configurado como puerta de enlace de conexión, los dispositivos administrados siempre tienen la opción de conectarse en forma directa con el Servidor de administración. Si sucede que la puerta de enlace no está disponible, pero establecer una conexión directa con el Servidor de administración es técnicamente posible, los dispositivos administrados se conectan directamente al Servidor de administración.

- Sondear la red para detectar nuevos dispositivos y actualizar la información disponible sobre los dispositivos de los que ya se tenía conocimiento. Un punto de distribución puede aplicar los mismos métodos de descubrimiento de dispositivos que el Servidor de administración.

- Instalar aplicaciones de Kaspersky y de terceros en forma remota utilizando las herramientas provistas por el sistema operativo del punto de distribución. El punto de distribución puede realizar instalaciones en dispositivos cliente que no cuentan con el Agente de red.

  Esta función permite transferir en forma remota paquetes de instalación del Agente de red a dispositivos cliente ubicados en redes a las que el Servidor de administración no tiene acceso.

- Actuar como servidor proxy vinculado a Kaspersky Security Network (KSN).

  Puede habilitar el servidor proxy de KSN en el punto de distribución para que el dispositivo actúe como proxy de KSN. En este caso, el servicio del proxy de KSN (ksnproxy) se ejecuta en el dispositivo.

La transmisión de archivos del Servidor de administración al punto de distribución se realiza mediante el protocolo HTTP o, si la conexión SSL está habilitada, el protocolo HTTPS. La utilización de HTTP o HTTPS genera un rendimiento más alto en comparación con SOAP, debido a la reducción de tráfico.

Los dispositivos con el Agente de red instalado pueden ser designados como puntos de distribución de forma manual (por el administrador) o automáticamente (por el Servidor de administración). La lista completa de puntos de distribución para los grupos de administración especificados se muestra en el informe sobre la lista de puntos de distribución.

El alcance de un punto de distribución se compone del grupo de administración para el que ha sido designado y de todos los subgrupos de ese grupo, sin límite de anidamiento. Cuando existe más de un punto de distribución en la jerarquía de grupos de administración, el Agente de red del dispositivo administrado se conecta con el punto de distribución que más cerca se encuentra en esa jerarquía.

El alcance de un punto de distribución también puede ser una ubicación de red. La ubicación de red se utiliza para crear manualmente el conjunto de dispositivos que reciben sus actualizaciones de un punto de distribución. Solo es posible determinar la ubicación de red de un dispositivo que utiliza el sistema operativo Windows.

Si el Servidor de administración asigna puntos de distribución automáticamente, los asigna por dominios de difusión, no por grupos de administración. Esto ocurre cuando se conocen todos los dominios de difusión. El Agente de red intercambia mensajes con otros Agentes de red en la misma subred y luego envía información al Servidor de administración acerca de sí mismo y los demás Agentes de red. El Servidor de administración puede usar esa información para agrupar los Agentes de red por dominios de difusión. El Servidor de administración conoce los dominios de difusión cuando sondea más del 70 % de los Agentes de red en los grupos de administración. El Servidor de administración sondea los dominios de difusión cada dos horas. Una vez que se asignan puntos de distribución mediante dominios de difusión, no se pueden reasignar por grupos de administración.

Si el administrador asigna manualmente puntos de distribución, se pueden asignar a grupos de administración o ubicaciones de red.

Los Agentes de red con el perfil de conexión activo no participan en la detección de dominios de difusión.

Kaspersky Security Center asigna a cada Agente de red una dirección de multidifusión IP única que se diferencia de todas las demás direcciones. Esto le permite evitar la sobrecarga de la red que podría ocurrir debido a superposiciones de IP.

Cuando hay dos o más puntos de distribución asignados a una misma área de red o a un mismo grupo de administración, uno de ellos se convierte en el punto de distribución activo y el restante (o los restantes) en punto(s) de distribución en espera. El punto de distribución activo descarga las actualizaciones y los paquetes de instalación directamente del Servidor de administración; los puntos de distribución en espera únicamente reciben actualizaciones del punto de distribución activo. Así, los archivos se descargan una sola vez del Servidor de administración y luego se distribuyen entre los puntos de distribución. Si el punto de distribución activo no se encuentra disponible por alguna razón, uno de los puntos de distribución en espera se vuelve activo. El Servidor de administración determina automáticamente que un punto de distribución debe quedar en espera.

El estado del punto de distribución (*Activo*/*En espera*) se muestra con una casilla en el informe klnagchk.

El punto de distribución debe tener un mínimo de 4 GB de espacio libre en su disco. Si el espacio libre en disco del punto de distribución es inferior a 2 GB, Kaspersky Security Center crea un problema de seguridad con el nivel de importancia *Advertencia*. El problema de seguridad se publicará en las propiedades del dispositivo, en la sección **Problemas de seguridad**.

La ejecución de tareas de instalación remotas en un dispositivo asignado como un punto de distribución requiere espacio libre adicional. El volumen de espacio libre debe superar el tamaño total de los paquetes de instalación que se instalarán.

La ejecución de tareas de actualización (instalación de parches) y de reparación de la vulnerabilidad en un dispositivo asignado como un punto de distribución requiere espacio libre adicional. El volumen de espacio libre debe ser de al menos el doble del tamaño total de los parches que se instalarán.

Los dispositivos designados como puntos de distribución deben protegerse contra el acceso no autorizado por medios virtuales y físicos.

# Puerta de enlace de conexión

Una *puerta de enlace de conexión* es un Agente de red que opera de un modo especial. Las puertas de enlace de conexión aceptan conexiones de otros agentes de red y las hacen llegar al Servidor de administración a través de la conexión que mantiene con el mismo. A diferencia de un Agente de red normal, una puerta de enlace de conexión no se encarga de establecer conexión con el Servidor de administración, sino que espera a que el Servidor de administración se conecte a ella.

Una puerta de enlace de conexión puede recibir conexiones de hasta 10 000 dispositivos.

Cuenta con dos opciones para utilizar las puertas de enlace de conexión:

- Le recomendamos que instale una puerta de enlace de conexión en una zona desmilitarizada (DMZ). En caso de otros agentes de red que estén instalados en dispositivos fuera de la oficina, debe configurar específicamente una conexión al Servidor de administración mediante la puerta de enlace de conexión.

  Una puerta de enlace de conexión no modifica ni procesa de ninguna manera los datos que se transmiten desde los Agentes de red al Servidor de administración. Además, no escribe los datos en ningún búfer y, por lo tanto, no puede aceptar datos de un Agente de red para luego reenviarlos al Servidor de administración. Si el Agente de red intenta conectarse al Servidor de administración mediante la puerta de enlace de conexión, pero esta no puede conectarse al Servidor de administración, el Agente de red lo percibe como si el Servidor de administración no estuviera accesible. Todos los datos permanecen en el Agente de red (no en la puerta de enlace de conexión).

  Una puerta de enlace de conexión no puede conectarse al Servidor de administración mediante otra puerta de enlace de conexión. Esto significa que el Agente de red no puede simultáneamente ser una puerta de enlace de conexión y utilizar una puerta de enlace de conexión para conectarse al Servidor de administración.

  En la lista de puntos de distribución en las propiedades del Servidor de administración, se incluyen todas las puertas de enlace de conexión.

- También puede utilizar puertas de enlace de conexión dentro de la red. Por ejemplo, los puntos de distribución asignados automáticamente también se convierten en puertas de enlace de conexión en su propio ámbito. Sin embargo, dentro de una red interna, las puertas de enlace de conexión no brindan un beneficio significativo. Reducen la cantidad de conexiones de red que recibe el Servidor de administración, pero no reducen el volumen de los datos entrantes. Incluso sin las puertas de enlace de conexión, todos los dispositivos podrían conectarse al Servidor de administración.

# Escenario de instalación principal

Siguiendo este escenario, puede desplegar el Servidor de administración, así como instalar el Agente de red y aplicaciones de seguridad en dispositivos en red. Puede seguir estos pasos solo para familiarizarse con la aplicación o para instalarla y seguir trabajando con ella.

La instalación de Kaspersky Security Center consta de los siguientes pasos:

1. Trabajo de preparación
2. Instalación de Kaspersky Security Center y una aplicación de seguridad de Kaspersky en el dispositivo del Servidor de administración
3. Despliegue centralizado de las aplicaciones de seguridad de Kaspersky en dispositivos cliente

El procedimiento para desplegar Kaspersky Security Center en un entorno de nube y el proceso para desplegar Kaspersky Security Center como proveedor de servicios se describen en otras secciones de la ayuda.

Recomendamos que asigne aproximadamente una hora para la instalación del Servidor de administración y un mínimo de un día hábil para la finalización del escenario. También recomendamos que instale una aplicación de seguridad, como Kaspersky Security for Windows Server o Kaspersky Endpoint Security, en el dispositivo que actuará como Servidor de administración de Kaspersky Security Center.

Una vez completado el escenario, la protección queda desplegada en la red de la organización de la siguiente manera:

- Se instala el DBMS para el Servidor de administración.
- Se instala el Servidor de administración de Kaspersky Security Center.
- Se crearán todas las directivas y las tareas requeridas; se especificarán las configuraciones predeterminadas de las directivas y las tareas.
- Se instalarán las aplicaciones de seguridad (por ejemplo, Kaspersky Endpoint Security para Windows) y el Agente de red en los dispositivos administrados.
- Se crearán los grupos de administración (pueden aparecer combinados en una jerarquía).
- Si es necesario, se desplegará la protección de dispositivos móviles.
- Se asignarán los puntos de distribución, si es necesario.

La instalación de Kaspersky Security Center se realiza en etapas:

## Trabajo de preparación

1. **Obtenga los archivos necesarios**

   Asegúrese de contar con una clave de licencia (código de activación) para Kaspersky Security Center o claves de licencia (códigos de activación) para las aplicaciones de seguridad de Kaspersky.

Desempaquete el archivo que recibió de su proveedor. Dentro del archivo, encontrará claves de licencia (archivos "KEY"), códigos de activación y una lista de las aplicaciones de Kaspersky que se pueden activar con cada clave de licencia.

Si primero desea probar Kaspersky Security Center, puede obtener una prueba gratuita de 30 días en el sitio web de Kaspersky.

Para obtener información detallada sobre las licencias de las aplicaciones de seguridad de Kaspersky que no forman parte de Kaspersky Security Center, consulte la documentación de esas aplicaciones.

2. **Selección de una estructura para la protección de organización**

Antes de nada, lea sobre los componentes de Kaspersky Security Center. Luego, seleccione la estructura de protección y la configuración de red que mejor se adapten a su organización. Basándose en la configuración de su red y en la capacidad de sus canales de comunicación, defina cuántos servidores de administración usará y cómo los distribuirá entre sus oficinas (si tiene una red distribuida).

Para lograr y mantener un rendimiento óptimo bajo condiciones de funcionamiento variables, tenga en cuenta el número de dispositivos conectados a la red, la topología de la red y el conjunto de funciones de Kaspersky Security Center que necesitará (para más información, consulte la Guía de dimensionamiento de Kaspersky Security Center).

Decida si usará una jerarquía de servidores de administración en su organización. Para hacer esto, debe evaluar si es posible y oportuno abarcar todos los dispositivos cliente con un solo Servidor de administración o si es necesario construir una jerarquía de Servidores de administración. También es posible que deba construir una jerarquía de Servidores de administración que sea idéntica a la estructura organizativa de la organización cuya red debe proteger.

Si necesita proteger dispositivos móviles, realice todas las acciones definidas como requisitos previos para configurar un Servidor de MDM para iOS.

Asegúrese de que los dispositivos que haya seleccionado como servidores de administración, así como aquellos en los que planee instalar la Consola de administración, cumplan con los requisitos de hardware y software.

3. **Preparación para el uso de certificados personalizados**

Si la infraestructura de claves públicas (PKI) de su organización exige el uso de certificados personalizados emitidos por una entidad de certificación (CA) específica, prepare esos certificados y asegúrese de que reúnan todos los requisitos.

4. **Preparación para la obtención de licencias de Kaspersky Security Center**

Si piensa usar una versión de Kaspersky Security Center con Administración de dispositivos móviles, Integración con sistemas SIEM y/o soporte de Administración de vulnerabilidades y parches, asegúrese de tener un archivo de clave o código de activación para la licencia de la aplicación.

5. **Prepare las licencias de las aplicaciones de seguridad administradas**

Durante el despliegue de la protección, deberá brindarle a Kaspersky las claves de licencia activas de las aplicaciones que desee administrar a través de Kaspersky Security Center (consulte la lista de aplicaciones de seguridad administrables). Para obtener información detallada sobre la licencia de cualquier aplicación de seguridad, puede consultar la documentación de la aplicación correspondiente.

6. **Selección de la configuración de hardware del Servidor de administración y DBMS**

Basándose en el número de dispositivos que haya en su red, planee la configuración de hardware que tendrán el Servidor de administración y el sistema de administración de bases de datos (DBMS).

7. **Selección de un DBMS**

A la hora de seleccionar un DBMS, tenga en cuenta el número de dispositivos administrados que cubrirá el Servidor de administración. Si su red tiene menos de 10 000 dispositivos y no piensa sobrepasar este número, puede elegir un DBMS gratuito, como SQL Express o MySQL, e instalarlo en el mismo dispositivo que el Servidor de administración. También puede optar por MariaDB, que le permitirá administrar hasta 20 000 dispositivos. Si su red tiene más de 10 000 dispositivos (o si planea expandirla hasta ese número de dispositivos), le recomendamos que elija un DBMS SQL que no sea gratuito y que lo instale en un equipo dedicado. Los DBMS pagos pueden operar con varios servidores de administración; los gratuitos, solamente con uno.

Si elige SQL Server como DBMS, tenga en cuenta que podrá migrar los datos almacenados en la base de datos a un DBMS MySQL, MariaDB o Azure SQL. Para realizar la migración, tendrá que crear una copia de seguridad de los datos y restaurarla en el nuevo DBMS.

### 8 Instale el DBMS y cree la base de datos

Lea sobre las cuentas que se necesitan para operar con un DBMS e instale el DBMS por el que se haya decidido.

Antes de la instalación, elija un DBMS compatible. Puede seleccionar, por ejemplo, PostgreSQL, Postgres Pro, Microsoft SQL Server, MySQL o MariaDB.

Para obtener información sobre cómo instalar el DBMS seleccionado, consulte su documentación.

Si decide instalar MariaDB, MySQL, PostgreSQL o Postgres Pro, use la configuración recomendada para garantizar que el DBMS funcione correctamente.

Anote y guarde la configuración de DBMS, ya que los necesitará durante la instalación del Servidor de administración. Esta configuración incluye el nombre de SQL Server, el número de puerto usado para la conexión a SQL Server, el nombre y la contraseña de la cuenta para acceder al equipo de SQL Server.

> Si decide instalar PostgreSQL o Postgres Pro, asegúrese de especificar la contraseña del superusuario. Si no especifica esta contraseña, es posible que el Servidor de administración no pueda conectarse a la base de datos.

De forma predeterminada, el instalador de Kaspersky Security Center se ocupa de crear la base de datos en la que se almacena la información del Servidor de administración. Puede optar por no crear esta base de datos y usar, en cambio, una base de datos diferente. En este caso, asegúrese de que la base de datos se haya creado, de saber cuál es su nombre, y de que la cuenta con la cual el Servidor de administración accederá a esta base de datos tenga la función db_owner para ello.

Si es necesario, póngase en contacto con su administrador de DBMS para obtener más información.

### 9 Configure los puertos

Asegúrese de que se encuentren abiertos todos los puertos necesarios para permitir la interacción de los componentes en la estructura de seguridad seleccionada.

Si tiene que brindar acceso a Internet al Servidor de administración, configure los puertos y defina los ajustes de conexión pertinentes para la configuración de su red.

### 10 Comprobación de cuentas

Asegúrese de tener todos los derechos de administrador local que necesite para instalar el Servidor de administración de Kaspersky Security Center y para desplegar luego la protección a los dispositivos. Los derechos de administrador local en los dispositivos cliente son necesarios para la instalación del Agente de red en estos dispositivos. Después de que se instala el Agente de red, puede usarlo para instalar aplicaciones en dispositivos remotamente, sin usar la cuenta con los derechos del administrador del dispositivo.

De forma predeterminada, en el dispositivo seleccionado para la instalación del Servidor de administración, el instalador de Kaspersky Security Center crea tres cuentas locales para ejecutar el Servidor de administración y los servicios de Kaspersky Security Center:

- KL-AK-*: Cuenta de servicio del Servidor de administración
- Servicio NT/KSC*: cuenta para otros servicios del grupo del Servidor de administración

- KlPxeUser: Cuenta para el despliegue de sistemas operativos

Puede optar por no crear cuentas para los servicios del Servidor de administración y otros servicios. Haga esto si prefiere usar cuentas que ya existan (cuentas de dominio, por ejemplo, si planea instalar el Servidor de administración en un clúster de conmutación por error o si, por algún otro motivo, prefiere usar cuentas de dominio en lugar de cuentas locales). En este caso, asegúrese de que las cuentas destinadas a ejecutar el Servidor de administración y los servicios de Kaspersky Security Center se hayan creado, no tengan privilegios y tengan todos los permisos necesarios para acceder al DBMS. (Si planea implementar más sistemas operativos en dispositivos a través de Kaspersky Security Center, no omita la creación de cuentas).

## Instalación de Kaspersky Security Center y una aplicación de seguridad de Kaspersky en el dispositivo del Servidor de administración

1. **Instale el Servidor de administración, la Consola de administración, Kaspersky Security Center Web Console y los complementos de administración para las aplicaciones de seguridad**

   Descargue Kaspersky Security Center del sitio web de Kaspersky. Puede descargar el paquete completo, solo Web Console o solo la consola de administración.

   Instale el Servidor de administración en el dispositivo seleccionado (o en los dispositivos seleccionados, si tiene pensado usar varios servidores de administración). Puede optar por realizar una instalación estándar o una instalación personalizada del Servidor de administración. La Consola de administración se instalará junto con el Servidor de administración. Se recomienda instalar el Servidor de administración en un servidor dedicado y no en un controlador de dominio.

   Recomendamos que realice una instalación estándar si lo que le interesa es probar Kaspersky Security Center (por ejemplo, si quiere evaluar el funcionamiento de la solución en una pequeña área de su red). Durante la instalación estándar, solo se configura la base de datos. También puede instalar solo el conjunto predeterminado de complementos de administración para las aplicaciones de Kaspersky. También puede utilizar la instalación estándar si ya tiene experiencia de trabajo con Kaspersky Security Center y sabe cómo especificar todas las configuraciones relevantes después de la instalación estándar.

   Recomendamos que realice una instalación personalizada si piensa hacer cambios de configuración en Kaspersky Security Center (por ejemplo, si planea cambiar la ruta de acceso a la carpeta compartida, los ajustes de la base de datos o las cuentas y los puertos que se usarán para conectarse al Servidor de administración). La instalación personalizada le permite especificar qué complementos de administración de Kaspersky instalar. Si es necesario, puede iniciar la instalación personalizada en el modo no interactivo.

   La Consola de administración y la versión del servidor del Agente de red se instalan junto con el Servidor de administración. Durante la instalación, también podrá instalar Kaspersky Security Center Web Console.

   Si desea operar con el Servidor de administración a través de la red, puede instalar la Consola de administración y/o Kaspersky Security Center Web Console por separado, en la estación de trabajo del administrador.

2. **Realice la configuración inicial y aplique las licencias**

   Cuando termine de instalar el Servidor de administración y se conecte a él por primera vez, se ejecutará automáticamente el asistente de inicio rápido. Realice la configuración inicial del Servidor de administración según los requisitos existentes. Durante la etapa de configuración inicial, el asistente usará los ajustes predeterminados para crear las directivas y tareas necesarias para desplegar la protección. Estos ajustes podrían no ser los ideales para su organización. De ser este el caso, podrá modificar la configuración de las directivas y las tareas (Configuración de la protección en la red de una organización cliente, Escenario: Configurar la protección de la red).

   Si planea utilizar funciones que van más allá de la funcionalidad básica, debe obtener una licencia para la aplicación. Podrá ocuparse de esto en uno de los pasos del Asistente de inicio rápido.

3. **Verifique que el Servidor de administración se haya instalado correctamente**

   Cuando todos los pasos anteriores se han completado, el Servidor de administración se instala y está listo para su uso.

Asegúrese de que la Consola de administración se esté ejecutando y pueda conectarse al Servidor de administración mediante la Consola de administración. Verifique, además, que la tarea "Descargar actualizaciones en el repositorio del Servidor de administración" esté disponible en el Servidor de administración (revise la carpeta **Tareas** del árbol de la consola). Controle también que exista una directiva para Kaspersky Endpoint Security (revise la carpeta **Directivas** del árbol de la consola).

De no haber inconvenientes, continúe con los siguientes pasos.

## Despliegue centralizado de las aplicaciones de seguridad de Kaspersky en dispositivos cliente

1. **Descubrimiento de dispositivos conectados a la red**

   Este paso es parte del Asistente de inicio rápido. El proceso de descubrimiento de dispositivos también se puede iniciar manualmente. Kaspersky Security Center recibe las direcciones y nombres de todos los dispositivos detectados en la red. Puede usar a continuación Kaspersky Security Center para instalar Aplicaciones de Kaspersky y software desde otros proveedores en los dispositivos detectados. Kaspersky Security Center realiza un descubrimiento de dispositivos periódicamente, lo que significa que si aparece alguna instancia nueva en la red, se la detectará automáticamente.

2. **Instalación del Agente de red y aplicaciones de seguridad en dispositivos en red**

   Desplegar la protección en la red de una organización (Configuración de la protección en la red de una organización cliente, Escenario: Configurar la protección de la red) implica instalar el Agente de red junto con Kaspersky Endpoint Security (u otras aplicaciones de seguridad) en los dispositivos detectados por el Servidor de administración durante el descubrimiento de dispositivos.

   Las aplicaciones de seguridad protegen los dispositivos frente a virus u otros programas que suponen una amenaza. El Agente de red garantiza la comunicación entre el dispositivo y el Servidor de administración. La configuración de Agente de red se ajusta automáticamente de forma predeterminada.

   Si lo desea, puede instalar el Agente de red en modo silencioso con un archivo de respuesta o sin usar un archivo de respuesta.

   Antes de iniciar la instalación del Agente de red y las aplicaciones de seguridad en los dispositivos de la red, asegúrese de que pueda acceder a estos dispositivos (es decir, que estén encendidos). Puede instalar el Agente de red tanto en máquinas virtuales como en dispositivos físicos.

   Las aplicaciones de seguridad y el Agente de red pueden instalarse en forma remota o local.

   Instalación remota: el Asistente de despliegue de la protección permite instalar la aplicación de seguridad (por ejemplo, Kaspersky Endpoint Security para Windows) y el Agente de red de manera remota en los dispositivos encontrados en la red de la organización por el Servidor de administración. Por lo general, la tarea de instalación remota logra desplegar la protección en la mayoría de los dispositivos conectados a una red. Sin embargo, puede devolver un error en algunos dispositivos si, por ejemplo, un dispositivo se desactiva o está inaccesible. En este caso, recomendamos que se conecte al dispositivo manualmente y use la instalación local.

   Instalación local: este método se utiliza en dispositivos conectados a la red que no se han podido proteger a través de la tarea de instalación remota. Para instalar la protección en dichos equipos, cree un paquete de instalación independiente que pueda ejecutar de forma local en esos dispositivos.

   La instalación del Agente de red en dispositivos con sistemas operativos Linux y macOS se describe en la documentación de Kaspersky Endpoint Security for Linux y Kaspersky Endpoint Security for Mac, respectivamente. Aunque los dispositivos con los sistemas operativos Linux y macOS se consideran menos vulnerables que los dispositivos con Windows, recomendamos que aun así instale aplicaciones de seguridad en dichos dispositivos.

   Después de la instalación, asegúrese de que la aplicación de seguridad esté instalada en los dispositivos administrados. Genere un informe de las versiones de software de Kaspersky y revise los resultados.

3. **Despliegue de claves de licencia a los dispositivos cliente**

   Despliegue claves de licencia a los dispositivos cliente para activar las aplicaciones de seguridad administradas en esos dispositivos.

4. **Configuración de protección de dispositivos móviles**

   Este paso es parte del Asistente de inicio rápido.

   Si desea administrar dispositivos móviles corporativos, encárguese de los preparativos pertinentes y despliegue la función de administración de dispositivos móviles.

5. **Creación de una estructura de grupo de administración**

   En algunos casos, para desplegar la protección en los dispositivos de la red con mayor facilidad, tendrá que repartir la totalidad de los dispositivos en grupos de administración con arreglo a la estructura de su organización. Puede crear reglas de movimiento que organicen los dispositivos en grupos por usted o puede distribuir los dispositivos manualmente. Puede asignar tareas de grupo para grupos de administración, definir el alcance de directivas y asignar puntos de distribución.

   Asegúrese de que todos los dispositivos administrados se hayan asignado correctamente a los grupos de administración apropiados y que no queden dispositivos no asignados en la red.

6. **Designar los puntos de distribución**

   Kaspersky Security Center asigna puntos de distribución a los grupos de administración automáticamente, pero usted puede asignarlos manualmente, si es necesario. Se recomienda usar puntos de distribución en redes de gran escala, pues ayudan a reducir la carga del Servidor de administración. También son recomendables en redes con una estructura distribuida, ya que pueden brindarle al Servidor de administración acceso a dispositivos (o grupos de dispositivos) que se comuniquen a través de canales con un ancho de banda limitado. Los puntos de distribución pueden ser dispositivos con Linux o con Windows.

# Puertos usados por Kaspersky Security Center

Las siguientes tablas muestran los puertos predeterminados que utilizan los Servidores de administración y los dispositivos cliente. Si lo desea, puede cambiar los números de puerto predeterminados.

Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo en el que se encuentre la base de datos (por ejemplo, el puerto 3306 para MySQL Server, el puerto 1433 para Microsoft SQL Server o el puerto 5432 para PostgreSQL y Postgres Pro). Consulte la documentación del DBMS para obtener la información necesaria.

Puertos utilizados por el Servidor de administración

| Número de puerto | Nombre del proceso que abre el puerto | Protocolo | Objetivo del puerto | Alcance |
|---|---|---|---|---|
| 8060 | klcsweb | TCP | Transmisión de paquetes de instalación publicados a dispositivos cliente | Publicación de paquetes de instalación.<br>Puede cambiar el número de puerto predeterminado en la sección **Servidor web** de la ventana de propiedades del Servidor de administración, que está disponible tanto en la Consola de administración como en Kaspersky Security Center Web Console.<br>Este puerto es opcional. Por razones de seguridad, recomendamos utilizar el puerto TCP 8061. |
| 8061 | klcsweb | TCP (TLS) | Transmisión de paquetes de instalación publicados a dispositivos cliente | Publicación de paquetes de instalación.<br>Puede cambiar el número de puerto predeterminado en la sección **Servidor web** de la ventana de propiedades del Servidor de administración, que está disponible tanto en la Consola de administración como en Kaspersky Security Center Web Console. |

| Número de puerto | Nombre del proceso que abre el puerto | Protocolo | Objetivo del puerto | Alcance |
|---|---|---|---|---|
| 13000 | klserver | TCP (TLS) | Recepción de conexiones de los agentes de red y de los servidores de administración secundarios. Los servidores de administración secundarios también usan este puerto para recibir conexiones del Servidor de administración principal (por ejemplo, si el Servidor de administración secundario está en una DMZ). | Administración de dispositivos cliente y servidores de administración secundarios.<br>Si desea cambiar el puerto que se usa por defecto para recibir conexiones de los Agentes de red, puede hacerlo al configurar los puertos de conexión; si desea cambiar el puerto que se usa por defecto para recibir conexiones de los servidores de administración secundarios, puede hacerlo al crear una jerarquía de servidores de administración mediante la Consola de administración o mediante Kaspersky Security Center Web Console. |
| 13000 | klserver | UDP | Recepción de información sobre dispositivos que se han apagado mediante los agentes de red | Administración de dispositivos cliente.<br>Puede cambiar el número de puerto predeterminado en los ajustes de la directiva del Agente de red en la Consola de administración o en Kaspersky Security Center Web Console. |
| 13291 | klserver | TCP (TLS) | Recepción de conexiones de la Consola de administración destinadas al Servidor de administración | Administración del Servidor de administración.<br>Puede cambiar el número de puerto predeterminado mediante la Consola de administración, a través de la ventana de propiedades del Servidor de administración. |
| 13299 | klserver | TCP (TLS) | Recepción de conexiones de Kaspersky Security Center Web Console destinadas al Servidor de administración; recepción de conexiones para el Servidor de administración realizadas mediante OpenAPI | Kaspersky Security Center Web Console, OpenAPI.<br>Puede cambiar el número de puerto predeterminado a través de la ventana de propiedades del Servidor de administración (sección **Configuración de conexión del Servidor de administración** → subsección **Puertos de conexión**) en la Consola de administración, o al crear una jerarquía de Servidores de administración en la Consola de administración o en Kaspersky Security Center Web Console. |
| 14000 | klserver | TCP | Recepción de conexiones de los agentes de red | Administración de dispositivos cliente.<br>Si desea cambiar el número de puerto predeterminado, puede hacerlo al configurar los puertos de conexión durante la instalación de Kaspersky Security Center o al momento de conectar un dispositivo cliente al Servidor de administración de forma manual.<br>Este puerto es opcional. Por razones de seguridad, recomendamos utilizar el puerto TCP 13000. |
| 13111 (solo si el servicio del proxy de KSN se ejecuta en el dispositivo) | ksnproxy | TCP | Recepción de solicitudes enviadas por los dispositivos administrados al servidor proxy de KSN | Servidor proxy de KSN.<br>Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración. |
| 15111 (solo si el servicio del proxy de KSN se ejecuta en el dispositivo) | ksnproxy | UDP | Recepción de solicitudes enviadas por los dispositivos administrados al servidor proxy de KSN | Servidor proxy de KSN.<br>Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración. |
| 17000 | klactprx | TCP (TLS) | Recepción de conexiones establecidas por los dispositivos administrados (excepto los móviles) para activar aplicaciones | Servidor proxy de activación utilizado por los dispositivos no móviles para activar las aplicaciones de Kaspersky con códigos de activación.<br>Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración. |
| 17100 (solo si administra dispositivos móviles) | klactprx | TCP (TLS) | Recepción de conexiones establecidas por los dispositivos móviles para activar aplicaciones | Servidor proxy de activación para dispositivos móviles.<br>Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración. |

| Número de puerto | Nombre del proceso que abre el puerto | Protocolo | Objetivo del puerto | Alcance |
|---|---|---|---|---|
| 19170 | klserver | HTTPS (TLS) | Túneles de conexión establecidos con la utilidad klsctunnel para comunicarse con los dispositivos administrados | Conexiones establecidas con dispositivos administrados remotos a través de Kaspersky Security Center Web Console.<br>Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración solo en la Consola de administración (sección **Configuración de conexión del Servidor de administración** → subsección **Puertos de conexión** → **Abrir puerto de RDP para Kaspersky Security Center Web Console**). |
| 13292 (solo si administra dispositivos móviles) | klserver | TCP (TLS) | Recepción de conexiones de dispositivos móviles | Administración de dispositivos móviles.<br>Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración en la Consola de administración o en Kaspersky Security Center Web Console. |
| 13294 (solo si administra dispositivos móviles) | klserver | TCP (TLS) | Recepción de conexiones de dispositivos con protección de UEFI | Administración de dispositivos cliente con protección de UEFI.<br>Puede cambiar el número de puerto predeterminado al conectar dispositivos móviles o, posteriormente, en la ventana de propiedades del Servidor de administración (sección **Configuración de conexión del Servidor de administración** → subsección **Puertos de conexión**) tanto en la Consola de administración como en Kaspersky Security Center Web Console. |
| 13296 | klserver | TCP (TLS) | Publicación de métricas de Kaspersky Security Center para Prometheus | Publicación de métricas de Kaspersky Security Center que Prometheus obtendrá.<br>Puede ver las métricas a través del siguiente vínculo: https://`<dirección_del_servidor>`:13296/metrics. En `<dirección_del_servidor>`, especifique la dirección IP o el nombre de dominio de su Servidor de administración.<br>Puede cambiar el número de puerto predeterminado en la Consola de administración, desde la ventana de propiedades del Servidor de administración. |
| 30522,<br>30523 (puertos en la interfaz de localhost) | klnagent | TCP | Recibir actualizaciones de la aplicación de Kaspersky desde el Servidor de administración mediante el componente FileTransferBridge | El dispositivo del Servidor de administración que recibe las actualizaciones de la aplicación de Kaspersky. |

La siguiente tabla muestra el puerto que utiliza el Servidor de MDM para iOS (solo si administra dispositivos móviles).

Puerto utilizado por el servidor de MDM para iOS

| Número de puerto | Nombre del proceso que abre el puerto | Protocolo | Objetivo del puerto | Alcance |
|---|---|---|---|---|
| 443 | kliosmdmservicesrv | TCP (TLS) | Recepción de conexiones de dispositivos móviles iOS | Administración de dispositivos móviles.<br>Puede cambiar el número de puerto predeterminado durante la instalación del Servidor de MDM para iOS. |

La siguiente tabla muestra el puerto que utiliza el servidor de Kaspersky Security Center Web Console. Este servidor puede estar en el mismo dispositivo que el Servidor de administración o en otro diferente.

Puerto usado por Kaspersky Security Center Web Console

| Número de puerto | Nombre del proceso que abre el puerto | Protocolo | Objetivo del puerto | Alcance |
|---|---|---|---|---|
| 8080 | Node.js: JavaScript del lado del servidor | TCP (TLS) | Recepción de conexiones del navegador web destinadas a Kaspersky Security Center Web Console | Kaspersky Security Center Web Console.<br>Puede cambiar el número de puerto predeterminado cuando instale Kaspersky Security Center Web Console en un dispositivo con Windows o en una plataforma Linux. Si instala Kaspersky Security Center Web Console en el sistema operativo Linux ALT, deberá indicar un número de puerto distinto del 8080: el puerto 8080 es utilizado por el sistema operativo. |

La siguiente tabla muestra el puerto que utilizan los dispositivos administrados en los que está instalado el Agente de red.

Puertos usados por el Agente de red

| Número de puerto | Nombre del proceso que abre el puerto | Protocolo | Objetivo del puerto | Alcance |
|---|---|---|---|---|
| 15000 | klnagent | UDP | Señales de administración enviadas del Servidor de administración o del Punto de distribución a los Agentes de red | Administración de dispositivos cliente.<br>Puede cambiar el número de puerto predeterminado en los ajustes de la directiva del Agente de red en la Consola de administración o en Kaspersky Security Center Web Console. |
| 15000 | klnagent | Difusión UDP | Obtención de datos sobre otros agentes de red dentro del mismo dominio de difusión (los datos se envían luego al Servidor de administración) | Distribución de actualizaciones y paquetes de instalación. |
| 15001 | klnagent | UDP | Recepción de solicitudes multidifusión de un punto de distribución (si se lo utiliza) | Recepción de actualizaciones y paquetes de instalación de un punto de distribución.<br>Puede cambiar el número de puerto predeterminado en la ventana de propiedades del punto de distribución en la Consola de administración o en Kaspersky Security Center Web Console. |
| 30522,<br>30523 (puertos en la interfaz de localhost) | klnagent | TCP | Recibir actualizaciones de la aplicación de Kaspersky desde el Servidor de administración mediante el componente FileTransferBridge | Dispositivos administrados que reciben actualizaciones de la aplicación de Kaspersky del Servidor de administración especificado como origen de actualizaciones de las bases de datos. |
| 161 | klnagent | SNMP | Supervisión y detección de dispositivos en red. | Detección de dispositivos. |

Tenga en cuenta que el proceso klnagent también puede solicitar puertos libres que pertenezcan al grupo de puertos dinámicos del sistema operativo instalado en el endpoint. El sistema operativo asigna estos puertos a klnagent en forma automática; por este motivo, el proceso klnagent podría tomar puertos utilizados por otras aplicaciones. Si el proceso klnagent afecta el funcionamiento de otras aplicaciones, cambie la configuración de puertos en esas aplicaciones o excluya los puertos afectados del grupo de puertos dinámicos del sistema operativo.

También tenga en cuenta que las recomendaciones sobre la compatibilidad de Kaspersky Security Center con software de terceros se describen solo como referencia y es posible que no se apliquen a nuevas versiones de software de terceros. Las recomendaciones descritas para configurar puertos se basan en las experiencias de Soporte técnico y en nuestras prácticas recomendadas.

La siguiente tabla muestra los puertos que utiliza un dispositivo administrado con Agente de red instalado actuando como punto de distribución. Los puertos enumerados los utilizan los dispositivos del punto de distribución además de los puertos utilizados por los Agentes de red (consulte la tabla anterior).

Puertos usados por el Agente de red cuando opera como punto de distribución

| Número de puerto | Nombre del proceso que abre el puerto | Protocolo | Objetivo del puerto | Alcance |
|---|---|---|---|---|
| 13000 | klnagent | TCP (TLS) | Recepción de conexiones de Agentes de red y de Kaspersky Security Center cuando el punto de distribución actúa como puerta de enlace de conexión en DMZ. Si se especifica un dispositivo con el Servidor de administración instalado como punto de distribución, el puerto 13001 se utiliza para la conexión SSL de forma predeterminada en lugar del 13000. | Administración de dispositivos cliente y distribución de actualizaciones y paquetes de instalación.<br>Para obtener más información, consulte el siguiente tema: Servidor de administración, una puerta de enlace de conexión en un segmento de red y un dispositivo cliente.<br>Puede cambiar el número de puerto predeterminado en la ventana de propiedades del punto de distribución en la Consola de administración o en Kaspersky Security Center Web Console. |
| 13111 (solo si el servicio del proxy de KSN se ejecuta en el dispositivo) | ksnproxy | TCP | Recepción de solicitudes enviadas por los dispositivos administrados al servidor proxy de KSN | Servidor proxy de KSN.<br>Puede cambiar el número de puerto predeterminado en la ventana de propiedades del punto de distribución en la Consola de administración o en Kaspersky Security Center Web Console. |
| 15111 (solo si el servicio del proxy de KSN se ejecuta en el dispositivo) | ksnproxy | UDP | Recepción de solicitudes enviadas por los dispositivos administrados al servidor proxy de KSN | Servidor proxy de KSN.<br>Puede cambiar el número de puerto predeterminado en la ventana de propiedades del punto de distribución en la Consola de administración o en Kaspersky Security Center Web Console. |
| 17111 (solo si el servicio del proxy de KSN se ejecuta en el dispositivo) | ksnproxy | HTTPS | Recepción de solicitudes enviadas por los dispositivos administrados al servidor proxy de KSN | Servidor proxy de KSN.<br>Puede cambiar el número de puerto predeterminado en la ventana de propiedades del punto de distribución en la Consola de administración o en Kaspersky Security Center Web Console. |
| 13295 (solo si utiliza el punto de distribución como servidor push) | klnagent | TCP (TLS) | Recepción de conexiones de dispositivos cliente | Servidor push.<br>Puede cambiar el número de puerto predeterminado en la ventana de propiedades del punto de distribución en la Consola de administración o en Kaspersky Security Center Web Console. |

La siguiente tabla muestra los puertos que utiliza un dispositivo controlador de dominio.

Puertos que utiliza un dispositivo controlador de dominio

| Número de puerto | Protocolo | Objetivo del puerto | Alcance |
|---|---|---|---|
| 389 | LDAP sobre TCP o UDP | Conexión a un servidor LDAP | Sondeo del controlador de dominio |
| 636 | LDAP sobre TLS | Conexión a un servidor LDAP | Sondeo del controlador de dominio |

# Certificados para trabajar con Kaspersky Security Center

En esta sección, se brinda información sobre los certificados de Kaspersky Security Center y se explica cómo emitir un certificado personalizado para el Servidor de administración.

# Acerca de los certificados de Kaspersky Security Center

Los siguientes tipos de certificados permiten que los componentes de Kaspersky Security Center interactúen en forma segura:

- Certificado del Servidor de administración
- Certificado para dispositivos móviles
- Certificado del Servidor de MDM para iOS
- Certificado del Servidor web de Kaspersky Security Center
- Certificado de Kaspersky Security Center Web Console

Los certificados que se utilizan por defecto son autofirmados, es decir, son certificados emitidos por el propio Kaspersky Security Center. Si así lo exigen los requisitos de su red o los estándares de seguridad de su organización, puede reemplazarlos por certificados personalizados. Los certificados personalizados asumen el mismo alcance funcional que los autofirmados una vez que el Servidor de administración ha verificado que cumplen con todos los requisitos. La única diferencia entre las dos clases de certificados es que los personalizados no se renuevan automáticamente al caducar. Para reemplazar certificados autofirmados por personalizados, deberá usar, según el tipo de certificado, la utilidad klsetsrvcert o la Consola de administración (específicamente, en este último caso, la sección de propiedades del Servidor de administración). Si decide usar la utilidad klsetsrvcert, utilice uno de los siguientes valores para indicar el tipo de certificado:

- C (certificado común para los puertos 13000 y 13291)
- CR (certificado común de reserva para los puertos 13000 y 13291)
- M (certificado para dispositivos móviles, para el puerto 13292)
- MR (certificado de reserva para dispositivos móviles, para el puerto 13292)
- MCA (entidad de certificación móvil para certificados de usuario autogenerados)

No necesita descargar la utilidad klsetsrvcert. Esta utilidad se incluye en el kit de distribución de Kaspersky Security Center. No es compatible con versiones más antiguas de Kaspersky Security Center.

El período máximo de validez para cualquiera de los certificados del Servidor de administración debe ser de 397 días o menos.

## Certificados del Servidor de administración

Se requiere un certificado del Servidor de administración para la autenticación del Servidor de administración, así como para la interacción segura entre el Servidor de administración y el Agente de red en los dispositivos administrados o entre el Servidor de administración principal y los Servidores de administración secundarios. La primera vez que se conecte al Servidor de administración con la Consola de administración, se le pedirá que confirme el uso del certificado del Servidor de administración vigente. Volverá a ver esta solicitud cuando el certificado se reemplace, si reinstala el Servidor de administración o si conecta un Servidor de administración secundario al Servidor de administración principal. El certificado del Servidor de administración se denomina certificado común ("C").

El certificado común ("C") se crea automáticamente cuando se instala el componente del Servidor de administración. El certificado tiene dos partes:

- Archivo klserver.cer; de forma predeterminada, se encuentra en el dispositivo donde está instalado el componente del Servidor de administración en la carpeta C:\ProgramData\KasperskyLab\adminkit\1093\cert.
- Clave secreta ubicada en el Almacenamiento protegido de Windows.

También existe un certificado común de reserva ("CR"). Kaspersky Security Center lo genera en forma automática 90 días antes de que caduque el certificado común. El certificado común de reserva se instala luego, de manera transparente, como nuevo certificado del Servidor de administración. Cuando el certificado común está próximo a caducar, el certificado de reserva se utiliza para mantener la conexión con las copias del Agente de red instaladas en los dispositivos administrados. Para tal fin, el certificado común de reserva se convierte en el nuevo certificado común 24 horas antes de que caduque el original.

Cabe destacar que el certificado del Servidor de administración se puede guardar en una copia de seguridad que no incluya ningún otro ajuste del Servidor. Esta facilidad permite mudar el Servidor de administración de un dispositivo a otro sin perder información.

## Certificados para dispositivos móviles

El certificado para dispositivos móviles ("M") permite autenticar el Servidor de administración en los dispositivos móviles. El uso de este certificado se configura a través del Asistente de inicio rápido, que dispone de un paso específico para ello.

También existe un certificado de reserva para dispositivos móviles ("MR"). Se lo utiliza para reemplazar, de manera simple, el certificado para dispositivos móviles. Kaspersky Security Center lo genera en forma automática 60 días antes de que caduque el certificado común. Cuando el certificado para dispositivos móviles está próximo a caducar, el certificado MR se utiliza para mantener la conexión con las instancias del Agente de red instaladas en los dispositivos administrados. Para tal fin, el certificado de reserva para dispositivos móviles se convierte en el nuevo certificado para dispositivos móviles 24 horas antes de que caduque el original.

Si el procedimiento de conexión requiere el uso de un certificado cliente en dispositivos móviles (conexión con autenticación SSL bidireccional), puede generar esos certificados mediante la autoridad de certificación para certificados de usuario generados automáticamente ("MCA"). El Asistente de inicio rápido le permitirá comenzar a usar certificados cliente personalizados que hayan sido emitidos por una entidad de certificación diferente. Con la capacidad de integrar la infraestructura de claves públicas (PKI) de su organización, podrá utilizar la entidad de certificación de su dominio para emitir los certificados cliente.

## Certificado del Servidor de MDM para iOS

El certificado del Servidor de MDM para iOS se utiliza para realizar la autenticación del Servidor de administración en los dispositivos móviles que utilizan el sistema operativo iOS. La interacción con estos equipos se lleva a cabo mediante el protocolo de administración de dispositivos móviles (MDM) definido por Apple. El mecanismo no requiere utilizar un Agente de red. Lo que se hace, en cambio, es instalar un perfil de MDM para iOS en cada dispositivo; el perfil contiene un certificado cliente, que permite realizar una autenticación SSL bidireccional.

El Asistente de inicio rápido le permitirá comenzar a usar certificados cliente personalizados que hayan sido emitidos por una entidad de certificación diferente. Con la capacidad de integrar la infraestructura de claves públicas (PKI) de su organización, podrá utilizar la entidad de certificación de su dominio para emitir los certificados cliente.

El dispositivo iOS obtiene su certificado cliente al descargar el perfil de MDM para iOS. Un certificado de cliente del servidor de MDM para iOS es único para cada dispositivo iOS administrado. Usted genera todos los certificados de cliente del Servidor de MDM para iOS mediante la autoridad de certificación para certificados de usuario generados automáticamente ("MCA").

## Certificado del Servidor web de Kaspersky Security Center

Kaspersky Security Center Web Server (en adelante, Web Server), un componente del Servidor de administración de Kaspersky Security Center, utiliza un tipo especial de certificado. Este certificado es necesario para publicar paquetes de instalación del Agente de red que posteriormente descargará en dispositivos administrados, así como para publicar perfiles de MDM para iOS, aplicaciones de iOS y paquetes de instalación de Kaspersky Security para dispositivos móviles. El Servidor web puede usar distintos certificados para tal fin.

Si la compatibilidad con dispositivos móviles no está habilitada, el Servidor web usará uno de los siguientes certificados (en orden de prioridad):

1. certificado personalizado, elegido manualmente para el Servidor web a través de la Consola de administración
2. certificado común del Servidor de administración ("C")

Si la compatibilidad con dispositivos móviles está habilitada, el Servidor web usará uno de los siguientes certificados (en orden de prioridad):

1. certificado personalizado, elegido manualmente para el Servidor web a través de la Consola de administración
2. Certificado para dispositivos móviles personalizado
3. certificado para dispositivos móviles autofirmado ("M")
4. certificado común del Servidor de administración ("C")

## Certificado de Kaspersky Security Center Web Console

El Servidor de Kaspersky Security Center Web Console (o también, en adelante, "Web Console") tiene su propio certificado. Cuando abre un sitio web, el navegador verifica si su conexión es fiable. El certificado de la consola web le permite autenticar la consola web y se utiliza para cifrar el tráfico entre el navegador y la consola web.

Cuando abre Web Console, el navegador le informa que la conexión a Web Console no es privada y que el certificado de Web Console no es válido. La advertencia se muestra porque Web Console utiliza un certificado autofirmado, generado automáticamente por Kaspersky Security Center. Para deshacerse de esta advertencia, realice una de las siguientes acciones:

- Reemplace el certificado de Web Console con uno personalizado (opción recomendada). Cree un certificado que sea de confianza en su infraestructura y que cumpla con los requisitos para certificados personalizados.
- Agregue el certificado de Web Console a la lista de certificados que el navegador considera de confianza. Recomendamos que utilice esta opción solo si no puede crear un certificado personalizado.

# Acerca del certificado del Servidor de administración

Se realizan dos operaciones en función del *Certificado del Servidor de administración:* la autenticación del Servidor de administración durante la conexión mediante la Consola de administración y el intercambio de datos con los dispositivos. El certificado también se utiliza para la autenticación cuando se conectan Servidores de administración principales a un Servidor de administración secundario.

## Certificado emitido por Kaspersky

El certificado del Servidor de administración se crea automáticamente durante la instalación del componente Servidor de administración y se almacena en la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

El certificado del Servidor de administración tendrá una validez de cinco años si se lo generó con la versión 12.2 o anterior del Servidor de administración. Si el certificado del Servidor de administración se emitió tras esa fecha, su validez será de solo 397 días. Cuando faltan 90 días para que el certificado activo caduque, el Servidor de administración genera uno nuevo y lo guarda como certificado de reserva. Posteriormente, el nuevo certificado sustituye automáticamente al certificado actual un día antes de la fecha de caducidad. Todos los agentes de red de los dispositivos cliente se reconfiguran automáticamente para autenticar el Servidor de administración con el nuevo certificado.

## Certificados personalizados

De ser necesario, puede asignarle un certificado personalizado al Servidor de administración. Por ejemplo, esto puede ser necesario para una mejor integración con la PKI existente de su empresa o para la configuración personalizada de los campos del certificado.

El período máximo de validez para cualquiera de los certificados del Servidor de administración debe ser de 397 días o menos.

Cuando reemplace el certificado, los agentes de red que estén conectados mediante SSL al Servidor de administración perderán su conexión y mostrarán un "error de autenticación del Servidor de administración". Para eliminar este error, deberá restaurar la conexión después de la sustitución del certificado.

Si el certificado del Servidor de administración se pierde, para recuperarlo, debe reinstalar el componente Servidor de administración y, luego, restaurar los datos.

Si abre Kaspersky Security Center Web Console en diferentes navegadores y descarga el archivo del certificado del Servidor de administración desde la ventana de propiedades del Servidor de administración, los archivos descargados tendrán nombres diferentes.

# Requisitos para los certificados personalizados que se utilizan en Kaspersky Security Center

En la siguiente tabla se enumeran los requisitos que deben reunir los certificados personalizados para los distintos componentes de Kaspersky Security Center.

Requisitos que deben reunir los certificados de Kaspersky Security Center

| Tipo de certificado | Requisitos | Comentarios |
|---|---|---|
| Certificado común, certificado de reserva común ("C", "CR") | Longitud mínima de la clave: 2048.<br>Restricciones básicas:<br>• Restricción de longitud de ruta: ninguna<br>Uso de claves:<br>• Firma digital<br>• Firma de certificados<br>• Cifrado de claves<br>• Firma de CRL<br>Uso extendido de claves (opcional): autenticación de servidor, autenticación de cliente. | El parámetro Extended Key Usage es opcional.<br>El valor de la restricción de longitud de ruta puede no ser "ninguna", pero en ese caso debe ser un número entero no inferior a 1. |
| Certificado móvil, Certificado de reserva móvil ("M", "MR") | Longitud mínima de la clave: 2048.<br>Restricciones básicas:<br>• CA: cierto<br>• Restricción de longitud de ruta: ninguna<br>Uso de claves:<br>• Firma digital<br>• Firma de certificados<br>• Cifrado de claves<br>• Firma de CRL<br>Extended Key Usage (opcional): autenticación de servidor. | El parámetro Extended Key Usage es opcional.<br>El valor de la restricción de longitud de ruta puede no ser "ninguna", pero en ese caso debe usarse un entero y el certificado común debe tener una restricción de longitud de ruta no inferior a 1. |
| CA de certificado para certificados de usuario generados automáticamente ("MCA") | Longitud mínima de la clave: 2048.<br>Restricciones básicas:<br>• CA: cierto<br>• Restricción de longitud de ruta: ninguna<br>Uso de claves:<br>• Firma digital<br>• Firma de certificados<br>• Cifrado de claves<br>• Firma de CRL<br>Uso extendido de claves (opcional): autenticación de servidor, autenticación de cliente. | El parámetro Extended Key Usage es opcional.<br>El valor de la restricción de longitud de ruta puede no ser "ninguna", pero en ese caso debe usarse un entero y el certificado común debe tener una restricción de longitud de ruta no inferior a 1. |

| Tipo de certificado | Requisitos | Comentarios |
| --- | --- | --- |
| Certificado del Servidor web | Uso extendido de clave: autenticación de servidor.<br>El contenedor PKCS #12 o PEM que se utilice para especificar el certificado debe incluir toda la cadena de claves públicas.<br>El nombre alternativo del sujeto (SAN) del certificado está presente; es decir, el valor del campo `subjectAltName` es válido.<br>El certificado debe ajustarse tanto a los requisitos que los navegadores exigen para los certificados de los servidores como a los requisitos básicos que ordena actualmente el CA/Browser Forum. | — |
| Certificado de Kaspersky Security Center Web Console | El contenedor PEM que se utilice para especificar el certificado debe incluir toda la cadena de claves públicas.<br>El nombre alternativo del sujeto (SAN) del certificado está presente; es decir, el valor del campo `subjectAltName` es válido.<br>El certificado debe ajustarse tanto a los requisitos que los navegadores exigen para los certificados de los servidores como a los requisitos básicos que ordena actualmente el CA/Browser Forum. | Kaspersky Security Center Web Console no es compatible con los certificados cifrados. |

# Escenario: Especificación del certificado del Servidor de administración personalizado

Puede asignar el certificado del Servidor de administración personalizado, por ejemplo, para una mejor integración con la infraestructura de claves públicas (PKI) existente de su empresa o para la configuración personalizada de los campos del certificado. Es conveniente reemplazar el certificado inmediatamente después de la instalación del Servidor de administración y antes de que el asistente de inicio rápido termine con sus operaciones.

El período máximo de validez para cualquiera de los certificados del Servidor de administración debe ser de 397 días o menos.

## Requisitos previos

Deben cumplirse las siguientes condiciones:

- El nuevo certificado debe crearse en formato PKCS#12 (por ejemplo, mediante la PKI de la organización).
- Para el nuevo certificado, se deben cumplir los requisitos que se enumeran en la siguiente tabla.

  En la siguiente tabla, preste atención al requisito "CA: true", que significa que el nuevo certificado debe ser emitido por una entidad de certificación (CA) de confianza. El nuevo certificado con el requisito "CA: true" debe incluir toda la cadena de confianza y una clave privada, que debe estar almacenada en un archivo con la extensión pfx o p12.

  Requisitos de los certificados del Servidor de administración

| Tipo de certificado | Requisitos |
| --- | --- |
| Certificado común, certificado de reserva común ("C", "CR") | Longitud mínima de la clave: 2048.<br>Restricciones básicas:<br>• Restricción de longitud de ruta: ninguna<br>El valor de la Restricción de longitud de ruta puede ser un número entero distinto de "Ninguna", pero no inferior a 1.<br>Uso de claves:<br>• Firma digital<br>• Firma de certificados<br>• Cifrado de claves<br>• Firma de CRL<br>Uso extendido de claves (EKU): autenticación del servidor y autenticación del cliente. El EKU es opcional, pero si su certificado lo contiene, los datos de autenticación del servidor y del cliente se deben especificar en el EKU. |
| Certificado móvil, Certificado de reserva móvil ("M", "MR") | Longitud mínima de la clave: 2048.<br>Restricciones básicas:<br>• CA: cierto<br>• Restricción de longitud de ruta: ninguna<br>El valor de la Restricción de longitud de ruta puede ser un número entero distinto de "Ninguna" si el certificado común tiene un valor de Restricción de longitud de ruta no inferior a 1.<br>Uso de claves:<br>• Firma digital<br>• Firma de certificados<br>• Cifrado de claves<br>• Firma de CRL<br>Uso extendido de claves (EKU): autenticación del servidor. El EKU es opcional, pero si su certificado lo contiene, los datos de autenticación del servidor se deben especificar en el EKU. |
| CA de certificado para certificados de usuario generados automáticamente ("MCA") | Longitud mínima de la clave: 2048.<br>Restricciones básicas:<br>• CA: cierto<br>• Restricción de longitud de ruta: ninguna<br>El valor de la Restricción de longitud de ruta puede ser un número entero distinto de "Ninguna" si el certificado Común tiene un valor de Restricción de longitud de ruta no inferior a 1.<br>Uso de claves:<br>• Firma digital<br>• Firma de certificados<br>• Cifrado de claves<br>• Firma de CRL<br>Uso extendido de claves (EKU): autenticación del cliente. El EKU es opcional, pero si su certificado lo contiene, los datos de autenticación del cliente se deben especificar en el EKU. |

Los certificados emitidos por una CA pública no tienen el permiso de firma de certificado. Para utilizar dichos certificados, asegúrese de haber instalado la versión 13 o superior del Agente de red en los puntos de distribución o puertas de enlace de conexión de su red. De lo contrario, no podrá utilizar certificados sin el permiso de firma.

### Etapas

La especificación del certificado del Servidor de administración se realiza por etapas:

1. **Reemplazo del certificado del Servidor de administración**

   Use la línea de comandos utilidad klsetsrvcert para este fin.

2. **Especificación de un nuevo certificado y restauración de la conexión de los Agentes de red al Servidor de administración**

   Al reemplazar el certificado, todos los Agentes de red que estaban conectados anteriormente al Servidor de administración a través de SSL pierden su conexión y devuelven "Error de autenticación del Servidor de administración". Para especificar el nuevo certificado y restaurar la conexión, use la línea de comandos utilidad klmover.

3. **Especificar un nuevo certificado en la configuración de Kaspersky Security Center Web Console**

   Después de reemplazar el certificado, especifíquelo en la configuración de Kaspersky Security Center Web Console. De lo contrario, Kaspersky Security Center Web Console no podrá conectarse con el Servidor de administración.

### Resultados

Al concluir el escenario, los Agentes de red reemplazan el certificado del Servidor de administración y autentican el servidor en los dispositivos administrados.

# Reemplazo del certificado del Servidor de administración mediante la utilidad klsetsrvcert

*Para reemplazar el certificado del Servidor de administración:*

Desde la línea de comandos, ejecute la siguiente utilidad:

```
klsetsrvcert [-t <tipo de certificado> {-i <ruta al certificado nuevo> [-p
<contraseña>] [-o <parámetros>] | -g <nombre dns>}][-f <hora de reemplazo>][-r
<certificados raíz>][-l <ruta de archivo de registro>]
```

No necesita descargar la utilidad klsetsrvcert. Esta utilidad se incluye en el kit de distribución de Kaspersky Security Center. No es compatible con versiones anteriores de Kaspersky Security Center.

La descripción de los parámetros de la utilidad klsetsrvcert se presenta en la siguiente tabla.

Valores de los parámetros de la utilidad klsetsrvcert

| Parámetro | Valor |
|---|---|
| `-t < tipo de certificado >` | Tipo del certificado para reemplazar. Valores posibles del parámetro `< tipo de certificado >`:<br>• `C`: reemplaza el certificado común para los puertos 13000 y 13291.<br>• `CR`: reemplaza el certificado de reserva común para los puertos 13000 y 13291.<br>• `M`: reemplazar el certificado para dispositivos móviles en el puerto 13292.<br>• `MR`: reemplazar el certificado de reserva en dispositivos móviles para el puerto 13292.<br>• `MCA`: CA de cliente móvil para certificados de usuario autogenerados. |
| `-f < tiempo de reemplazo >` | Horario para cambiar el certificado, utilizando el formato "DD-MM-YYYY hh:mm" (para los puertos 13000 y 13291).<br>Utilice este parámetro si desea reemplazar el certificado común con el certificado de reserva común antes de que caduque.<br>Especifique la hora en que los dispositivos administrados deben sincronizarse con el Servidor de administración en un nuevo certificado. |
| `-i < ruta al nuevo certificado >` | Contenedor con el certificado y una clave privada en formato PKCS#12 (archivo con extensión .p12 o .pfx). |
| `-p < contraseña >` | Contraseña utilizada para la protección del contenedor p12.<br>El certificado y la clave privada se almacenan en el contenedor, por lo tanto, se requiere la contraseña para descifrar el archivo con el contenedor. |
| `-o < parámetros de validación >` | Parámetros de validación del certificado (separados por punto y coma).<br>Para utilizar un certificado personalizado sin permiso de firma, especifique `-o NoCA` en la utilidad klsetsrvcert. Esto es útil para los certificados emitidos por una CA pública.<br>Para cambiar la longitud de la clave de cifrado para los tipos de certificado C o CR, especifique `-o RsaKeyLen: < longitud de la clave >` en la utilidad klsetsrvcert, donde el parámetro `< longitud de la clave >` es el valor de longitud de clave requerido. De lo contrario, se utiliza la longitud actual de la clave del certificado. |
| `-g < nombre del dns >` | Un nuevo certificado se creará para el nombre de DNS especificado. |
| `-r < certificados raíz >` | Lista de autoridades de certificación raíz de confianza, formato PEM. |
| `-l < ruta del archivo de registro >` | Archivo de salida de resultados. De forma predeterminada, la salida se redirige en la corriente de la salida estándar. |

Por ejemplo, para especificar el certificado del Servidor de administración personalizado, use el siguiente comando:

```
klsetsrvcert -t C -i <ruta al certificado nuevo> -p <contraseña> -o NoCA
```

Después de reemplazar el certificado, todos los Agentes de red conectados al Servidor de administración a través de SSL pierden su conexión. Para restaurarlo, use la línea de comando utilidad klmover.

Para que no se pierdan las conexiones de los agentes de red, use los siguientes comandos:

1. Para instalar el nuevo certificado,

   ```
   klsetsrvcert.exe -t CR -i <ruta al certificado nuevo> -p <contraseña> -o NoCA
   ```

2. Para especificar la fecha en que se aplicará el nuevo certificado,

   ```
   klsetsrvcert.exe -f "DD-MM-YYYY hh:mm"
   ```

dónde "`DD-MM-YYYY hh:mm`" es la fecha 3-4 semanas posterior a la fecha actual. Al modificar el momento para cambiar el certificado por el nuevo, dará tiempo a que el nuevo certificado se distribuya a la totalidad de los agentes de red.

# Conexión de los Agentes de red al Servidor de administración mediante la utilidad klmover

Después de reemplazar el certificado del Servidor de administración mediante la línea de comando utilidad klsetsrvcert, debe establecer la conexión SSL entre los Agentes de red y el Servidor de administración, ya que la conexión está interrumpida.

*Para especificar el nuevo certificado del Servidor de administración y restaurar la conexión:*

Desde la línea de comandos, ejecute la siguiente utilidad:

```
klmover [-address <dirección del servidor>] [-pn <número de puerto>] [-ps <número de puerto SSL>] [-nossl] [-cert <ruta al archivo de certificado>]
```

Se requieren derechos de administrador para ejecutar la utilidad.

Esta utilidad se copia automáticamente en la carpeta de instalación del Agente de red, cuando el Agente de red está instalado en un dispositivo cliente.

Para evitar que los intrusos muevan los dispositivos fuera del control de su Servidor de administración, recomendamos que active la protección con contraseña para ejecutar la utilidad klmover. Para habilitar la protección con contraseña, seleccione la opción **Utilizar contraseña de desinstalación** en la configuración de la directiva del Agente de red.

La utilidad klmover requiere derechos de administrador local. La protección con contraseña para ejecutar la utilidad klmover se puede omitir para dispositivos que funcionan sin derechos de administrador local.

Al activar la opción **Utilizar contraseña de desinstalación**, también se activa la protección con contraseña para la herramienta Cleaner (cleaner.exe).

No se puede utilizar la utilidad klmover para dispositivos cliente conectados al Servidor de administración mediante puertas de enlace de conexión. Para estos dispositivos, debe reconfigurar el Agente de red o reinstalar el Agente de red y especificar la puerta de enlace de conexión.

La descripción de los parámetros de la utilidad klmover se presenta en la siguiente tabla.

Valores de los parámetros de la utilidad de klmover

| Parámetro | Valor |
|---|---|
| `-address <dirección del servidor>` | Dirección del Servidor de administración para la conexión.<br>Puede especificar una dirección IP, el nombre NetBIOS o el nombre DNS. |
| `-pn <número de puerto>` | Número del puerto a través del cual se establece la conexión no cifrada con el Servidor de administración.<br>El número de puerto predeterminado es 14000. |
| `-ps <número de puerto SSL>` | número del puerto SSL a través del cual se establece la conexión al Servidor de administración, utilizando SSL.<br>El número de puerto predeterminado es 13000. |

| Parámetro | Valor |
| --- | --- |
| `-nossl` | usar conexión no cifrada al Servidor de administración.<br>Si la clave no está en uso, el Agente de red se conecta al Servidor de administración mediante el protocolo cifrado SSL. |
| `-cert < ruta al archivo del certificado >` | usa el archivo de certificado especificado para la autenticación del acceso al Servidor de administración. |
| `-virtserv` | Nombre del Servidor de administración virtual. |
| `-cloningmode` | Modo de clonación de disco del Agente de red.<br>Use uno de los siguientes parámetros para configurar el modo de clonación de disco:<br>• `-cloningmode`: solicitar el estado del modo de clonación de disco.<br>• `-cloningmode 1`: habilitar el modo de clonación de disco.<br>• `-cloningmode 0`: deshabilitar el modo de clonación de disco. |
| `-nauninstpwd < contraseña >` | Utilice este parámetro para especificar la contraseña de desinstalación del Agente de red.<br>El parámetro no es obligatorio. |

Por ejemplo, para conectar el Agente de red al Servidor de administración, ejecute el siguiente comando:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

# Volver a emitir el certificado del Servidor web

El certificado del Servidor web que se utiliza en Kaspersky Security Center es necesario para publicar paquetes de instalación del Agente de red que posteriormente descargará en dispositivos administrados, así como para publicar perfiles de MDM para iOS, aplicaciones de iOS y paquetes de instalación de Kaspersky Endpoint Security para dispositivos móviles. Según la configuración actual de la aplicación, varios certificados pueden funcionar como certificado del Servidor web (para obtener más detalles, consulte Acerca de los certificados de Kaspersky Security Center).

Es posible que deba volver a emitir el certificado del Servidor web para cumplir con los requisitos de seguridad específicos de su organización o para mantener la conexión continua de sus dispositivos administrados antes de comenzar a actualizar la aplicación. Kaspersky Security Center ofrece dos formas de volver a emitir el certificado del Servidor web; la elección entre los dos métodos depende de si tiene dispositivos móviles conectados y administrados a través del protocolo móvil (es decir, mediante el uso del certificado para dispositivos móviles).

Si nunca ha especificado su propio certificado personalizado como certificado del Servidor web en la sección **Servidor web** de la ventana de propiedades del Servidor de administración, el certificado para dispositivos móviles actúa como el certificado del Servidor Web. En este caso, para volver a emitir el certificado del Servidor web, se debe volver a emitir el protocolo móvil.

*Para volver a emitir el certificado del Servidor web cuando no tenga dispositivos móviles administrados a través del protocolo móvil, haga lo siguiente:*

1. En el árbol de la consola, haga clic con el botón derecho en el nombre del Servidor de administración correspondiente y, en el menú contextual, seleccione **Propiedades**.

2. En la ventana de propiedades del Servidor de administración que se abre, en el panel izquierdo seleccione la sección **Configuración de conexión del Servidor de administración**.

3. En la lista de subsecciones, seleccione la subsección **Certificados**.

4. Si planea continuar usando el certificado emitido por Kaspersky Security Center, haga lo siguiente:

   a. En el panel derecho, en el grupo de ajustes **Autenticación del Servidor de administración por dispositivos móviles**, seleccione la opción **Certificado emitido usando mediante el Servidor de administración** y haga clic en el botón **Emitir nuevamente**.

   b. En la ventana emergente **Emitir el certificado nuevamente**, en el grupo de ajustes **Dirección de conexión** y **Plazo de activación**, seleccione las opciones relevantes y haga clic en **Aceptar**.

   c. En la ventana de confirmación, haga clic en **Sí**.

   Como alternativa, si planea usar su propio certificado personalizado, haga lo siguiente:

   a. Compruebe si su certificado personalizado cumple los requisitos de Kaspersky Security Center y los requisitos de certificados de confianza de Apple. Si es necesario, modifique el certificado.

   b. Seleccione la opción **Otro certificado** y haga clic en el botón **Examinar**.

   c. En la ventana emergente **Certificado**, en el campo **Tipo de certificado** seleccione el tipo de su certificado y luego especifique la ubicación y la configuración del certificado:

      - Si seleccionó **Contenedor PKCS #12**, haga clic en el botón **Examinar** al lado del campo **Archivo del certificado** y especifique el archivo de certificado en su disco duro. Si el archivo del certificado está protegido con contraseña, ingrese la contraseña en el campo **Contraseña (si hay)**.

      - Si seleccionó **Certificado X.509**, haga clic en el botón **Examinar** al lado del campo **Clave privada (.prk, .pem)** y especifique la clave privada en su disco duro. Si la clave privada está protegida con contraseña, ingrese la contraseña en el campo **Contraseña (si hay)**. Luego haga clic en el botón **Examinar** al lado del campo **Clave pública (.cer)** y especifique la clave privada en su disco duro.

   d. En la ventana **Certificado**, haga clic **Aceptar**.

   e. En la ventana de confirmación, haga clic en **Sí**.

   El certificado para dispositivos móviles se vuelve a emitir para que se lo utilice como certificado del Servidor web.

*Para volver a emitir el certificado del Servidor web cuando tenga dispositivos móviles administrados a través del protocolo móvil, haga lo siguiente:*

1. Genere su certificado personalizado y prepárelo para su uso en Kaspersky Security Center. Compruebe si su certificado personalizado cumple los requisitos de Kaspersky Security Center y los requisitos de certificados de confianza de Apple. Si es necesario, modifique el certificado.

   > Puede utilizar la utilidad kliossrvcertgen.exe para generar los certificados.

2. En el árbol de la consola, haga clic con el botón derecho en el nombre del Servidor de administración correspondiente y, en el menú contextual, seleccione **Propiedades**.

3. En la ventana de propiedades del Servidor de administración que se abre, en el panel izquierdo seleccione la sección **Servidor web**.

4. En el menú **Sobre HTTPS**, seleccione la opción **Especificar otro certificado**.

5. En el menú **Sobre HTTPS**, haga clic en el botón **Cambiar**.

6. En la ventana emergente **Certificado**, en el campo **Tipo de certificado** seleccione el tipo de su certificado:

   - Si seleccionó **Contenedor PKCS #12**, haga clic en el botón **Examinar** al lado del campo **Archivo del certificado** y especifique el archivo de certificado en su disco duro. Si el archivo del certificado está protegido con contraseña, ingrese la contraseña en el campo **Contraseña (si hay)**.

   - Si seleccionó **Certificado X.509**, haga clic en el botón **Examinar** al lado del campo **Clave privada (.prk, .pem)** y especifique la clave privada en su disco duro. Si la clave privada está protegida con contraseña, ingrese la contraseña en el campo **Contraseña (si hay)**. Luego haga clic en el botón **Examinar** al lado del campo **Clave pública (.cer)** y especifique la clave privada en su disco duro.

7. En la ventana **Certificado**, haga clic en **Aceptar**.

8. Si es necesario, en la ventana de propiedades del Servidor de administración, en el campo **Puerto HTTPS del Servidor web** cambie el número del puerto HTTPS para el Servidor web. Haga clic en **Aceptar**.

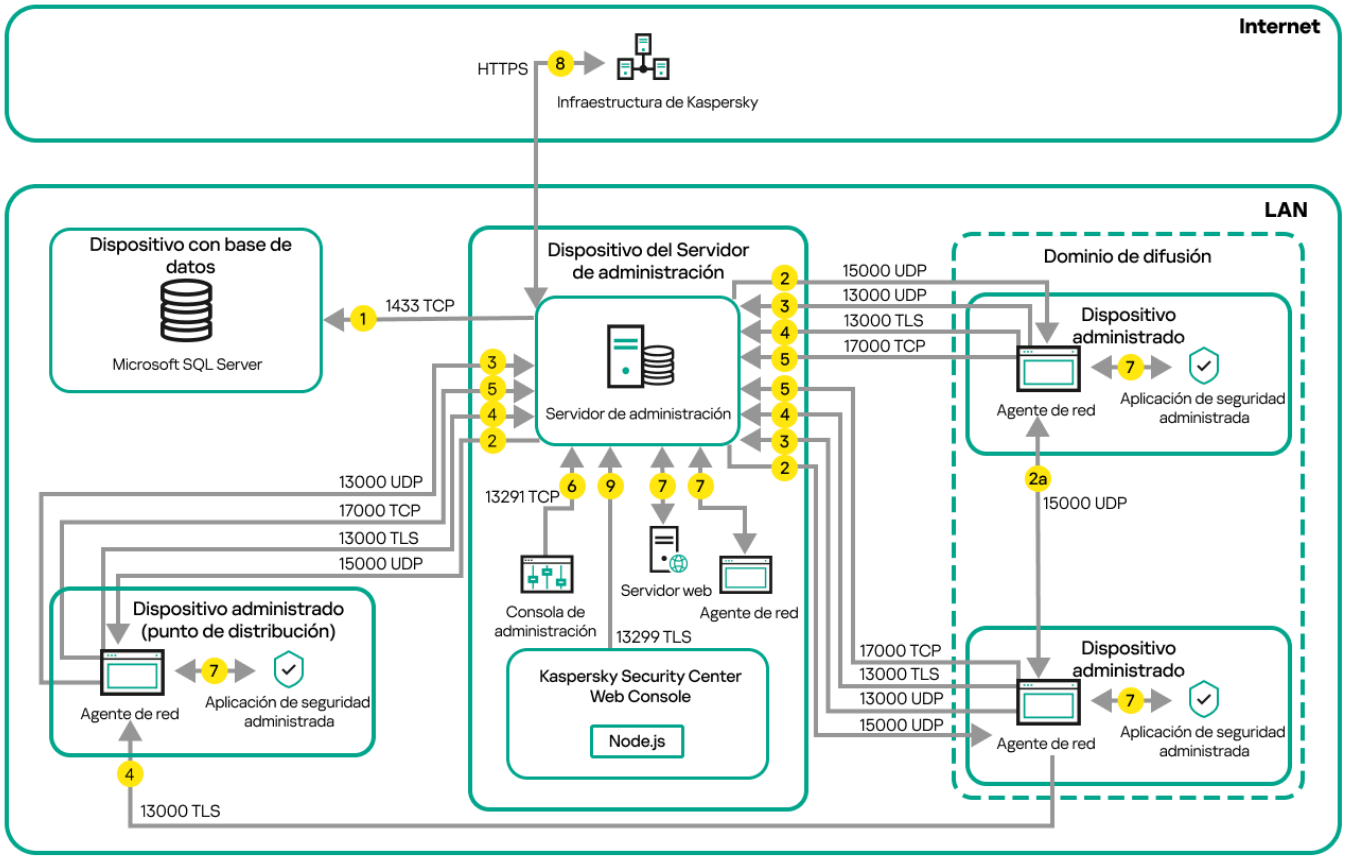
   Se volverá a emitir el certificado del Servidor web.

# Esquemas del tráfico de datos y de los puertos utilizados

En esta sección encontrará una serie de esquemas en los que se representa el tráfico de datos entre los componentes de Kaspersky Security Center, las aplicaciones de seguridad administradas y los servidores externos bajo distintas configuraciones. Los esquemas tienen numerados los puertos que deben estar disponibles en los dispositivos locales.

# Servidor de administración y dispositivos administrados en una LAN

La siguiente imagen es una representación del tráfico de datos cuando Kaspersky Security Center se ha desplegado únicamente en una red de área local (LAN).




Servidor de administración y dispositivos administrados en una red de área local (LAN)

La figura muestra cómo los diferentes dispositivos administrados se conectan al Servidor de administración de diferentes maneras: directamente o a través de un punto de distribución. Los puntos de distribución reducen la carga en el Servidor de administración durante la distribución de actualizaciones y optimizan el tráfico de red. Sin embargo, los puntos de distribución solo son necesarios si la cantidad de dispositivos administrados es lo suficientemente grande. Si la cantidad de dispositivos administrados es pequeña, todos los dispositivos administrados pueden recibir actualizaciones del Servidor de administración directamente.

Las flechas indican el inicio del tráfico: cada flecha apunta desde un dispositivo que inicia la conexión al dispositivo que "responde" a la llamada. También contienen el número de puerto y el nombre del protocolo con que se transfiere la información. Los números con los que están etiquetadas las flechas se corresponden con los tipos de tráfico que se detallan a continuación:

1. El Servidor de administración envía información a la base de datos. Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo en el que se encuentra la base de datos (por ejemplo, el puerto 3306 para MySQL Server o el puerto 1433 para Microsoft SQL Server). Consulte la documentación del DBMS para obtener la información necesaria.

2. Cuando el Servidor de administración necesita comunicarse con los dispositivos administrados no móviles, envía la solicitud correspondiente a través del puerto UDP 15000.

   Los agentes de red se envían solicitudes entre sí dentro de un dominio de transmisión. Luego, los datos se envían al Servidor de administración y se utilizan para definir los límites del dominio de transmisión y para la asignación automática de puntos de distribución (si esta opción está activada).

   Si el Servidor de administración no tiene acceso directo a los dispositivos administrados, las solicitudes de comunicación del Servidor de administración a estos dispositivos no se envían directamente.

3. Cuando un dispositivo administrado se apaga, el Agente de red se lo comunica al Servidor de administración a través del puerto UDP 13000.

4. Los Agentes de red y los Servidores de administración secundarios se conectan con el Servidor de administración a través del puerto TLS 13000.

   Si usó una versión anterior de Kaspersky Security Center, el Servidor de administración de su red puede recibir conexiones de Agentes de red a través del puerto (no de TLS) 14000. Kaspersky Security Center también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto TLS 13000.

   > En las versiones anteriores de Kaspersky Security Center, los puntos de distribución se denominaban "agentes de actualización".

5. Los dispositivos administrados (exceptuados los dispositivos móviles) envían sus solicitudes de activación a través del puerto TCP 17000. Esto solo es necesario cuando los dispositivos no tienen acceso propio a Internet; cuando pueden hacerlo, los dispositivos envían los datos directamente a los servidores de Kaspersky por Internet.

6. Los datos de la Consola de administración basada en MMC se transfieren al Servidor de administración a través del puerto 13291. (La Consola de administración se puede instalar en el mismo dispositivo o en otro).

7. Las aplicaciones instaladas en un mismo dispositivo intercambian tráfico local (esto es válido tanto para el Servidor de administración como para los dispositivos administrados). No se deben abrir puertos externos.

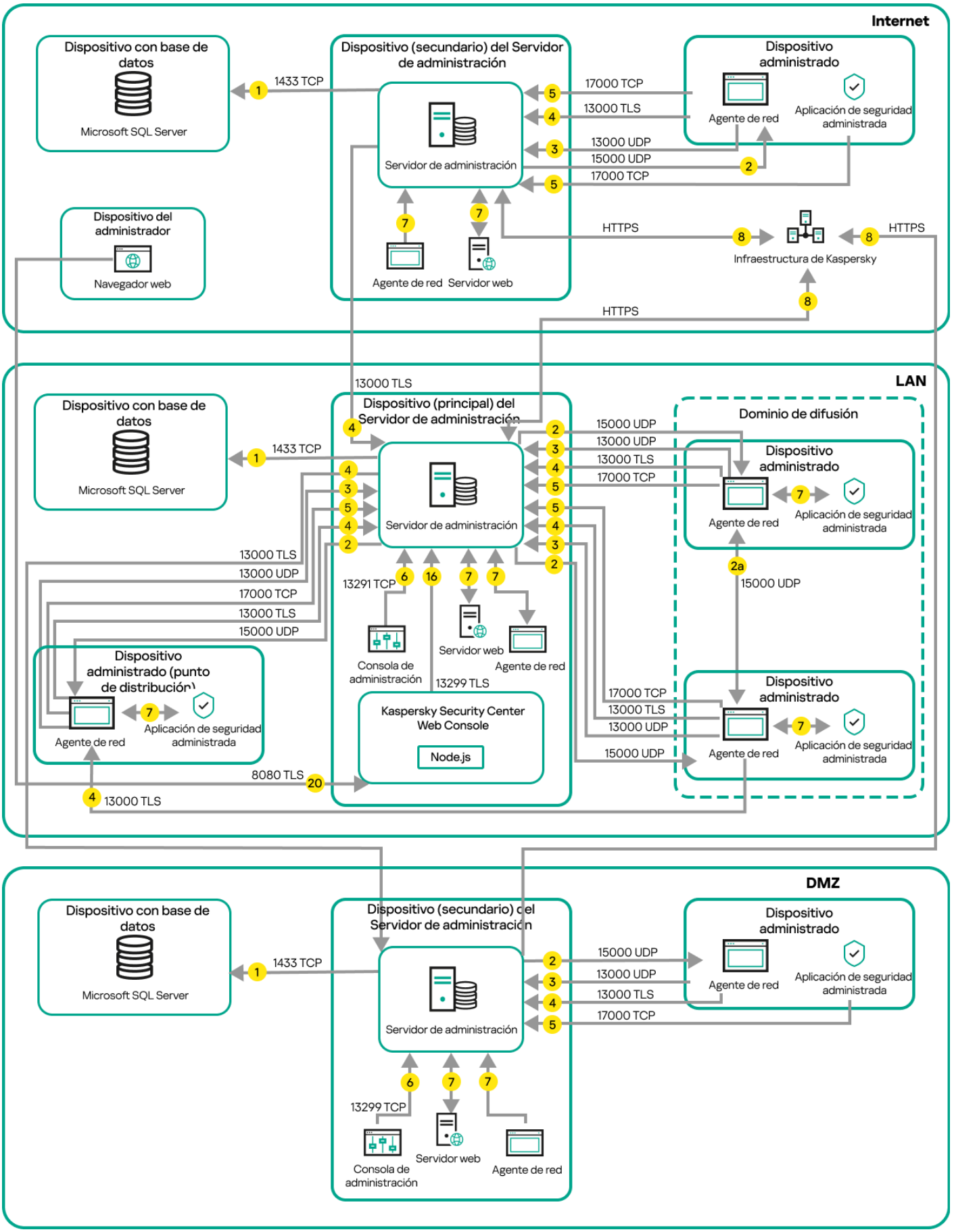
8. Los datos del Servidor de administración a los servidores de Kaspersky (como los datos de KSN o la información sobre licencias) y los datos de los servidores de Kaspersky al Servidor de administración (como las actualizaciones de aplicaciones y las actualizaciones de las bases de datos antivirus) se transfieren mediante el protocolo HTTPS.

   Si no quiere que el Servidor de administración tenga acceso a Internet, deberá administrar estos datos manualmente.

9. El Servidor de Kaspersky Security Center Web Console utiliza el puerto TLS 13299 para comunicarse con el Servidor de administración, que puede estar instalado en el mismo dispositivo o en otro separado.

# Servidor de administración principal en una LAN y dos Servidores de administración secundarios

La siguiente imagen es una representación de la jerarquía de Servidores de administración. El Servidor de administración principal se encuentra en una red de área local. Hay un Servidor de administración secundario en la zona desmilitarizada (DMZ) y otro Servidor de administración secundario en Internet.




Jerarquía de Servidores de administración: Servidor de administración principal y dos Servidores de administración secundarios

Las flechas indican el inicio del tráfico: cada flecha apunta desde un dispositivo que inicia la conexión al dispositivo que "responde" a la llamada. También contienen el número de puerto y el nombre del protocolo con que se transfiere la información. Los números con los que están etiquetadas las flechas se corresponden con los tipos de tráfico que se detallan a continuación:

1. El Servidor de administración envía información a la base de datos. Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo en el que se encuentra la base de datos (por ejemplo, el puerto 3306 para MySQL Server o el puerto 1433 para Microsoft SQL Server). Consulte la documentación del DBMS para obtener la información necesaria.

2. Cuando el Servidor de administración necesita comunicarse con los dispositivos administrados no móviles, envía la solicitud correspondiente a través del puerto UDP 15000.

   Los agentes de red se envían solicitudes entre sí dentro de un dominio de transmisión. Luego, los datos se envían al Servidor de administración y se utilizan para definir los límites del dominio de transmisión y para la asignación automática de puntos de distribución (si esta opción está activada).

   Si el Servidor de administración no tiene acceso directo a los dispositivos administrados, las solicitudes de comunicación del Servidor de administración a estos dispositivos no se envían directamente.

3. Cuando un dispositivo administrado se apaga, el Agente de red se lo comunica al Servidor de administración a través del puerto UDP 13000.

4. Los Agentes de red y los Servidores de administración secundarios se conectan con el Servidor de administración a través del puerto TLS 13000.

   Si usó una versión anterior de Kaspersky Security Center, el Servidor de administración de su red puede recibir conexiones de Agentes de red a través del puerto (no de TLS) 14000. Kaspersky Security Center también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto TLS 13000.

   > En las versiones anteriores de Kaspersky Security Center, los puntos de distribución se denominaban "agentes de actualización".

5. Los dispositivos administrados (exceptuados los dispositivos móviles) envían sus solicitudes de activación a través del puerto TCP 17000. Esto solo es necesario cuando los dispositivos no tienen acceso propio a Internet; cuando pueden hacerlo, los dispositivos envían los datos directamente a los servidores de Kaspersky por Internet.

6. Los datos de la Consola de administración basada en MMC se transfieren al Servidor de administración a través del puerto 13291. (La Consola de administración se puede instalar en el mismo dispositivo o en otro).

7. Las aplicaciones instaladas en un mismo dispositivo intercambian tráfico local (esto es válido tanto para el Servidor de administración como para los dispositivos administrados). No se deben abrir puertos externos.

8. Los datos del Servidor de administración a los servidores de Kaspersky (como los datos de KSN o la información sobre licencias) y los datos de los servidores de Kaspersky al Servidor de administración (como las actualizaciones de aplicaciones y las actualizaciones de las bases de datos antivirus) se transfieren mediante el protocolo HTTPS.

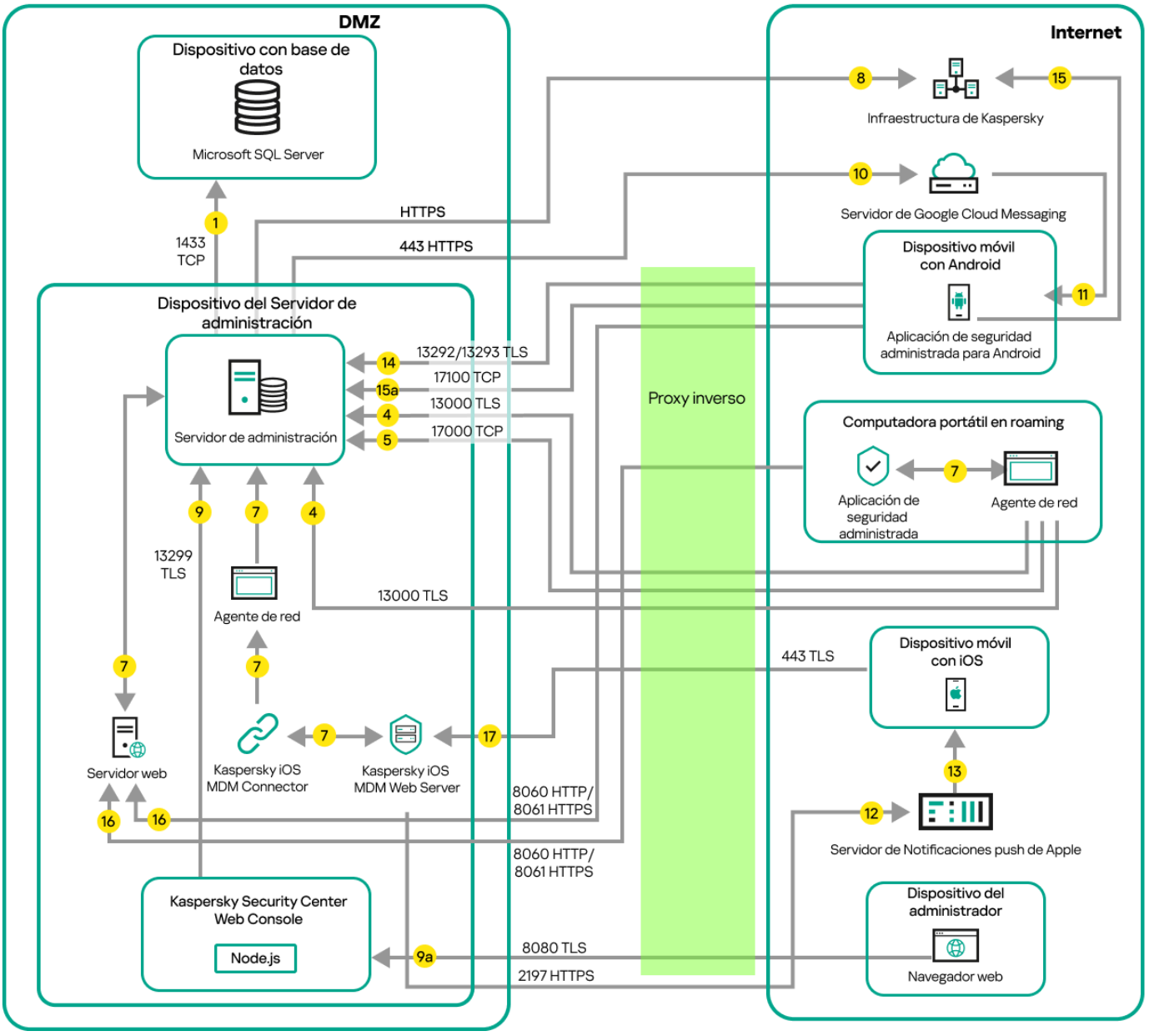
   Si no quiere que el Servidor de administración tenga acceso a Internet, deberá administrar estos datos manualmente.

9. El Servidor de Kaspersky Security Center Web Console utiliza el puerto TLS 13299 para comunicarse con el Servidor de administración, que puede estar instalado en el mismo dispositivo o en otro separado.

   9a. El tráfico del navegador, instalado en un dispositivo independiente que utiliza el administrador, se transfiere al Servidor de Kaspersky Security Center Web Console a través del puerto TLS 8080. El Servidor de Kaspersky Security Center Web Console se puede instalar en el mismo dispositivo que el Servidor de administración o en uno separado.

# Servidor de administración en una LAN, dispositivos administrados en Internet, se usa un proxy inverso

La siguiente imagen es una representación del tráfico de datos cuando el Servidor de administración está ubicado en una red de área local (LAN) y los dispositivos administrados, incluidos los dispositivos móviles, están en Internet. En esta figura, se está utilizando un proxy inverso de su elección. Consulte la documentación de la aplicación para obtener más información.




Servidor de administración en una red de área local; los dispositivos administrados se conectan con el Servidor de administración a través de un proxy inverso

Recomendamos que siga este esquema de despliegue cuando los dispositivos móviles no deban conectarse en forma directa con el Servidor de administración y no quiera asignar una puerta de enlace de conexión dentro de la DMZ.

Las flechas indican el inicio del tráfico: cada flecha apunta desde un dispositivo que inicia la conexión al dispositivo que "responde" a la llamada. También contienen el número de puerto y el nombre del protocolo con que se transfiere la información. Los números con los que están etiquetadas las flechas se corresponden con los tipos de tráfico que se detallan a continuación:

1. El Servidor de administración envía información a la base de datos. Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo en el que se encuentra la base de datos (por ejemplo, el puerto 3306 para MySQL Server o el puerto 1433 para Microsoft SQL Server). Consulte la documentación del DBMS para obtener la información necesaria.

2. Cuando el Servidor de administración necesita comunicarse con los dispositivos administrados no móviles, envía la solicitud correspondiente a través del puerto UDP 15000.

   Los agentes de red se envían solicitudes entre sí dentro de un dominio de transmisión. Luego, los datos se envían al Servidor de administración y se utilizan para definir los límites del dominio de transmisión y para la asignación automática de puntos de distribución (si esta opción está activada).

   Si el Servidor de administración no tiene acceso directo a los dispositivos administrados, las solicitudes de comunicación del Servidor de administración a estos dispositivos no se envían directamente.

3. Cuando un dispositivo administrado se apaga, el Agente de red se lo comunica al Servidor de administración a través del puerto UDP 13000.

4. Los Agentes de red y los Servidores de administración secundarios se conectan con el Servidor de administración a través del puerto TLS 13000.

   Si usó una versión anterior de Kaspersky Security Center, el Servidor de administración de su red puede recibir conexiones de Agentes de red a través del puerto (no de TLS) 14000. Kaspersky Security Center también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto TLS 13000.

   > En las versiones anteriores de Kaspersky Security Center, los puntos de distribución se denominaban "agentes de actualización".

5. Los dispositivos administrados (exceptuados los dispositivos móviles) envían sus solicitudes de activación a través del puerto TCP 17000. Esto solo es necesario cuando los dispositivos no tienen acceso propio a Internet; cuando pueden hacerlo, los dispositivos envían los datos directamente a los servidores de Kaspersky por Internet.

6. Los datos de la Consola de administración basada en MMC se transfieren al Servidor de administración a través del puerto 13291. (La Consola de administración se puede instalar en el mismo dispositivo o en otro).

7. Las aplicaciones instaladas en un mismo dispositivo intercambian tráfico local (esto es válido tanto para el Servidor de administración como para los dispositivos administrados). No se deben abrir puertos externos.

8. Los datos del Servidor de administración a los servidores de Kaspersky (como los datos de KSN o la información sobre licencias) y los datos de los servidores de Kaspersky al Servidor de administración (como las actualizaciones de aplicaciones y las actualizaciones de las bases de datos antivirus) se transfieren mediante el protocolo HTTPS.

   Si no quiere que el Servidor de administración tenga acceso a Internet, deberá administrar estos datos manualmente.

9. El Servidor de Kaspersky Security Center Web Console utiliza el puerto TLS 13299 para comunicarse con el Servidor de administración, que puede estar instalado en el mismo dispositivo o en otro separado.

   9a. El tráfico del navegador, instalado en un dispositivo independiente que utiliza el administrador, se transfiere al Servidor de Kaspersky Security Center Web Console a través del puerto TLS 8080. El Servidor de Kaspersky Security Center Web Console se puede instalar en el mismo dispositivo que el Servidor de administración o en uno separado.

10. Dispositivos móviles Android únicamente: el Servidor de administración se comunica con los servidores de Google. La conexión se utiliza para indicar a los dispositivos móviles Android que deben conectarse con el Servidor de administración. Las notificaciones push se envían entonces a los dispositivos móviles.

11. Dispositivos móviles Android únicamente: las notificaciones push de los servidores de Google se envían al dispositivo móvil. La conexión se utiliza para indicar a los dispositivos móviles que deben conectarse con el Servidor de administración.

12. Dispositivos móviles iOS únicamente: el Servidor de MDM para iOS se comunica con los servidores de notificaciones push de Apple. Las notificaciones push se envían entonces a los dispositivos móviles.

13. Solo para dispositivos móviles iOS: las notificaciones push se envían desde los servidores de Apple al dispositivo móvil. La conexión se utiliza para indicar a los dispositivos móviles iOS que deben conectarse con el Servidor de administración.

14. Dispositivos móviles únicamente: los datos de la aplicación administrada se transfieren al Servidor de administración (o a la puerta de enlace de conexión) a través de los puertos TLS 13292 o 13293, ya sea en forma directa o a través de un proxy inverso.

15. Dispositivos móviles únicamente: datos enviados por el dispositivo móvil a la infraestructura de Kaspersky.

    Si el dispositivo móvil no tiene acceso a Internet, el tráfico se envía primero al Servidor de administración a través del puerto 17100 y el Servidor de administración lo remite a los servidores de Kaspersky. Esta, sin embargo, no es una situación usual.

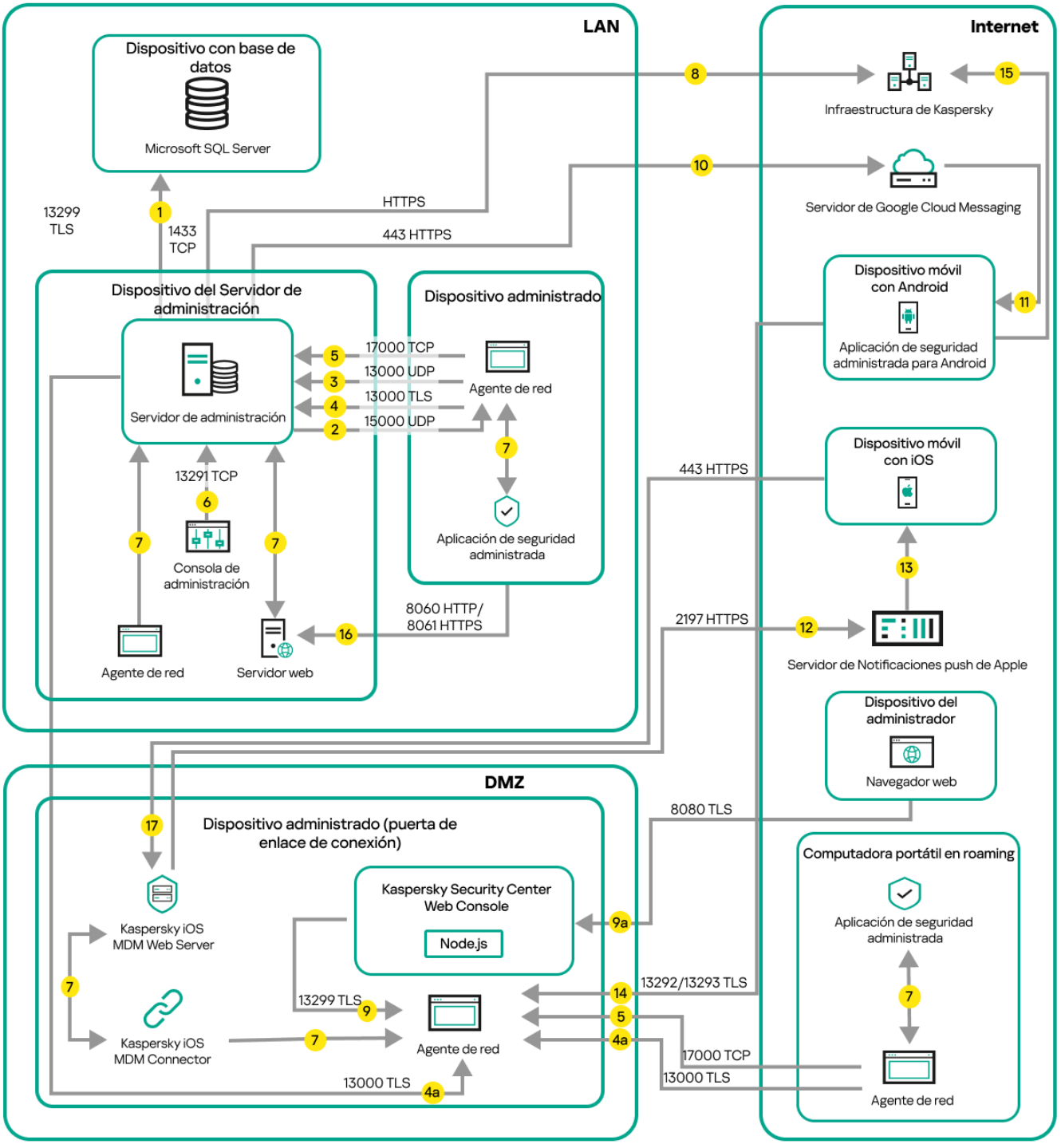
16. Las solicitudes de paquetes de los dispositivos administrados, incluidos los dispositivos móviles, se transfieren al Servidor web, que se encuentra en el mismo dispositivo que el Servidor de administración.

17. Solo para dispositivos móviles iOS: los datos de los dispositivos móviles se transfieren a través del puerto TLS 443 al servidor de MDM para iOS, que se encuentra en el mismo dispositivo que el Servidor de administración o en la puerta de enlace de conexión.

## Servidor de administración en una LAN, dispositivos administrados en Internet, se usa una puerta de enlace de conexión

La siguiente imagen es una representación del tráfico de datos cuando el Servidor de administración está ubicado en una red de área local (LAN) y los dispositivos administrados, incluidos los dispositivos móviles, están en Internet. Se utiliza una puerta de enlace de conexión.

Se recomienda este esquema de despliegue si no desea que los dispositivos móviles se conecten directamente al Servidor de administración ni desea usar un proxy inverso o un firewall corporativo.




Dispositivos móviles administrados que se conectan al Servidor de administración a través de una puerta de enlace de conexión

En la imagen de arriba, los dispositivos administrados se conectan con el Servidor de administración a través de una puerta de enlace de conexión, la cual se encuentra en una DMZ. No se utiliza ni un proxy inverso ni un firewall corporativo.

Las flechas indican el inicio del tráfico: cada flecha apunta desde un dispositivo que inicia la conexión al dispositivo que "responde" a la llamada. También contienen el número de puerto y el nombre del protocolo con que se transfiere la información. Los números con los que están etiquetadas las flechas se corresponden con los tipos de tráfico que se detallan a continuación:

1. El Servidor de administración envía información a la base de datos. Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo en el que se encuentra la base de datos (por ejemplo, el puerto 3306 para MySQL Server o el puerto 1433 para Microsoft SQL Server). Consulte la documentación del DBMS para obtener la información necesaria.

2. Cuando el Servidor de administración necesita comunicarse con los dispositivos administrados no móviles, envía la solicitud correspondiente a través del puerto UDP 15000.

   Los agentes de red se envían solicitudes entre sí dentro de un dominio de transmisión. Luego, los datos se envían al Servidor de administración y se utilizan para definir los límites del dominio de transmisión y para la asignación automática de puntos de distribución (si esta opción está activada).

   Si el Servidor de administración no tiene acceso directo a los dispositivos administrados, las solicitudes de comunicación del Servidor de administración a estos dispositivos no se envían directamente.

3. Cuando un dispositivo administrado se apaga, el Agente de red se lo comunica al Servidor de administración a través del puerto UDP 13000.

4. Los Agentes de red y los Servidores de administración secundarios se conectan con el Servidor de administración a través del puerto TLS 13000.

   Si usó una versión anterior de Kaspersky Security Center, el Servidor de administración de su red puede recibir conexiones de Agentes de red a través del puerto (no de TLS) 14000. Kaspersky Security Center también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto TLS 13000.

   > En las versiones anteriores de Kaspersky Security Center, los puntos de distribución se denominaban "agentes de actualización".

   4a. Si existe una puerta de enlace de conexión en la DMZ, también recibe las conexiones del Servidor de administración a través del puerto TLS 13000. El Servidor de administración crea y mantiene una conexión permanente —denominada conexión de señal— con la puerta de enlace. Esto es necesario porque la puerta de enlace, al encontrarse en la DMZ, no puede acceder a los puertos del Servidor. La conexión de señal no se utiliza para transferir información, sino para que una parte le indique a la otra que desea entablar un contacto de red sucesivo. Cuando la puerta de enlace necesita conectarse con el Servidor de administración, se lo hace saber a través de esta conexión; el Servidor, tras recibir este aviso, establece una conexión que permite el intercambio de datos.

   Los dispositivos que se encuentran fuera de la oficina también utilizan el puerto TLS 13000 para conectarse con la puerta de enlace de conexión.

5. Los dispositivos administrados (exceptuados los dispositivos móviles) envían sus solicitudes de activación a través del puerto TCP 17000. Esto solo es necesario cuando los dispositivos no tienen acceso propio a Internet; cuando pueden hacerlo, los dispositivos envían los datos directamente a los servidores de Kaspersky por Internet.

6. Los datos de la Consola de administración basada en MMC se transfieren al Servidor de administración a través del puerto 13291. (La Consola de administración se puede instalar en el mismo dispositivo o en otro).

7. Las aplicaciones instaladas en un mismo dispositivo intercambian tráfico local (esto es válido tanto para el Servidor de administración como para los dispositivos administrados). No se deben abrir puertos externos.

8. Los datos del Servidor de administración a los servidores de Kaspersky (como los datos de KSN o la información sobre licencias) y los datos de los servidores de Kaspersky al Servidor de administración (como las actualizaciones de aplicaciones y las actualizaciones de las bases de datos antivirus) se transfieren mediante el protocolo HTTPS.

   Si no quiere que el Servidor de administración tenga acceso a Internet, deberá administrar estos datos manualmente.

9. El Servidor de Kaspersky Security Center Web Console utiliza el puerto TLS 13299 para comunicarse con el Servidor de administración, que puede estar instalado en el mismo dispositivo o en otro separado.

   9a. El tráfico del navegador, instalado en un dispositivo independiente que utiliza el administrador, se transfiere al Servidor de Kaspersky Security Center Web Console a través del puerto TLS 8080. El Servidor de Kaspersky Security Center Web Console se puede instalar en el mismo dispositivo que el Servidor de administración o en uno separado.

10. Dispositivos móviles Android únicamente: el Servidor de administración se comunica con los servidores de Google. La conexión se utiliza para indicar a los dispositivos móviles Android que deben conectarse con el Servidor de administración. Las notificaciones push se envían entonces a los dispositivos móviles.

11. Dispositivos móviles Android únicamente: las notificaciones push de los servidores de Google se envían al dispositivo móvil. La conexión se utiliza para indicar a los dispositivos móviles que deben conectarse con el Servidor de administración.

12. Dispositivos móviles iOS únicamente: el Servidor de MDM para iOS se comunica con los servidores de notificaciones push de Apple. Las notificaciones push se envían entonces a los dispositivos móviles.

13. Solo para dispositivos móviles iOS: las notificaciones push se envían desde los servidores de Apple al dispositivo móvil. La conexión se utiliza para indicar a los dispositivos móviles iOS que deben conectarse con el Servidor de administración.

14. Dispositivos móviles únicamente: los datos de la aplicación administrada se transfieren al Servidor de administración (o a la puerta de enlace de conexión) a través de los puertos TLS 13292 o 13293, ya sea en forma directa o a través de un proxy inverso.

15. Dispositivos móviles únicamente: datos enviados por el dispositivo móvil a la infraestructura de Kaspersky.

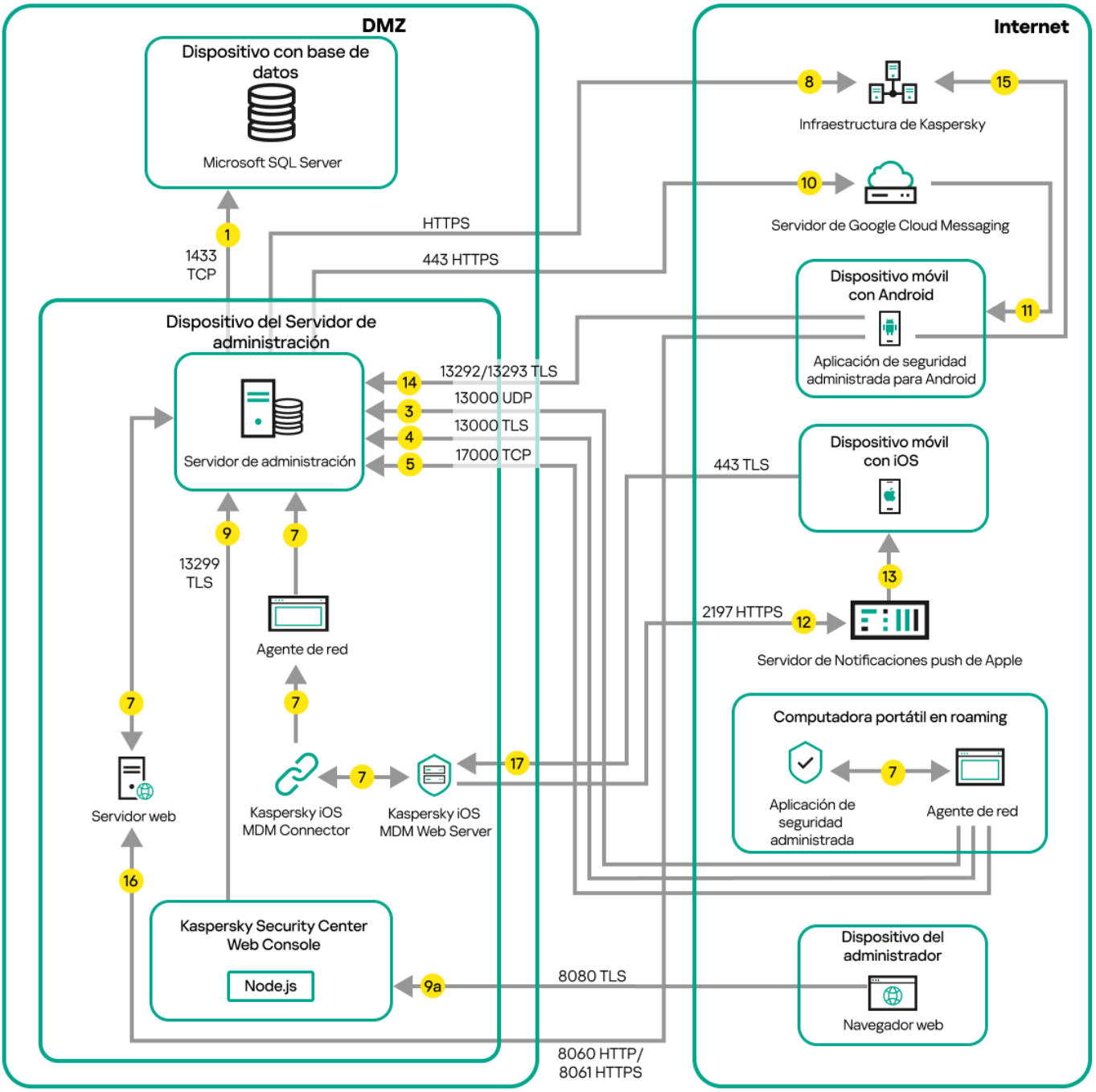
    Si el dispositivo móvil no tiene acceso a Internet, el tráfico se envía primero al Servidor de administración a través del puerto 17100 y el Servidor de administración lo remite a los servidores de Kaspersky. Esta, sin embargo, no es una situación usual.

16. Las solicitudes de paquetes de los dispositivos administrados, incluidos los dispositivos móviles, se transfieren al Servidor web, que se encuentra en el mismo dispositivo que el Servidor de administración.

17. Solo para dispositivos móviles iOS: los datos de los dispositivos móviles se transfieren a través del puerto TLS 443 al servidor de MDM para iOS, que se encuentra en el mismo dispositivo que el Servidor de administración o en la puerta de enlace de conexión.

# Servidor de administración en una DMZ, dispositivos administrados en Internet

La siguiente imagen es una representación del tráfico de datos cuando el Servidor de administración está ubicado en una zona desmilitarizada (DMZ) y los dispositivos administrados, incluidos los dispositivos móviles, están en Internet.




Servidor de administración en la DMZ, dispositivos móviles administrados en Internet

En el esquema de la imagen, no se utiliza una puerta de enlace de conexión; los dispositivos móviles establecen una conexión directa con el Servidor de administración.

Las flechas indican el inicio del tráfico: cada flecha apunta desde un dispositivo que inicia la conexión al dispositivo que "responde" a la llamada. También contienen el número de puerto y el nombre del protocolo con que se transfiere la información. Los números con los que están etiquetadas las flechas se corresponden con los tipos de tráfico que se detallan a continuación:

1. El Servidor de administración envía información a la base de datos. Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo en el que se encuentra la base de datos (por ejemplo, el puerto 3306 para MySQL Server o el puerto 1433 para Microsoft SQL Server). Consulte la documentación del DBMS para obtener la información necesaria.

2. Cuando el Servidor de administración necesita comunicarse con los dispositivos administrados no móviles, envía la solicitud correspondiente a través del puerto UDP 15000.

   Los agentes de red se envían solicitudes entre sí dentro de un dominio de transmisión. Luego, los datos se envían al Servidor de administración y se utilizan para definir los límites del dominio de transmisión y para la asignación automática de puntos de distribución (si esta opción está activada).

   Si el Servidor de administración no tiene acceso directo a los dispositivos administrados, las solicitudes de comunicación del Servidor de administración a estos dispositivos no se envían directamente.

3. Cuando un dispositivo administrado se apaga, el Agente de red se lo comunica al Servidor de administración a través del puerto UDP 13000.

4. Los Agentes de red y los Servidores de administración secundarios se conectan con el Servidor de administración a través del puerto TLS 13000.

   Si usó una versión anterior de Kaspersky Security Center, el Servidor de administración de su red puede recibir conexiones de Agentes de red a través del puerto (no de TLS) 14000. Kaspersky Security Center también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto TLS 13000.

   > En las versiones anteriores de Kaspersky Security Center, los puntos de distribución se denominaban "agentes de actualización".

5. Los dispositivos administrados (exceptuados los dispositivos móviles) envían sus solicitudes de activación a través del puerto TCP 17000. Esto solo es necesario cuando los dispositivos no tienen acceso propio a Internet; cuando pueden hacerlo, los dispositivos envían los datos directamente a los servidores de Kaspersky por Internet.

6. Los datos de la Consola de administración basada en MMC se transfieren al Servidor de administración a través del puerto 13291. (La Consola de administración se puede instalar en el mismo dispositivo o en otro).

7. Las aplicaciones instaladas en un mismo dispositivo intercambian tráfico local (esto es válido tanto para el Servidor de administración como para los dispositivos administrados). No se deben abrir puertos externos.

8. Los datos del Servidor de administración a los servidores de Kaspersky (como los datos de KSN o la información sobre licencias) y los datos de los servidores de Kaspersky al Servidor de administración (como las actualizaciones de aplicaciones y las actualizaciones de las bases de datos antivirus) se transfieren mediante el protocolo HTTPS.

   Si no quiere que el Servidor de administración tenga acceso a Internet, deberá administrar estos datos manualmente.

9. El Servidor de Kaspersky Security Center Web Console utiliza el puerto TLS 13299 para comunicarse con el Servidor de administración, que puede estar instalado en el mismo dispositivo o en otro separado.

   9a. El tráfico del navegador, instalado en un dispositivo independiente que utiliza el administrador, se transfiere al Servidor de Kaspersky Security Center Web Console a través del puerto TLS 8080. El Servidor de Kaspersky Security Center Web Console se puede instalar en el mismo dispositivo que el Servidor de administración o en uno separado.

10. Dispositivos móviles Android únicamente: el Servidor de administración se comunica con los servidores de Google. La conexión se utiliza para indicar a los dispositivos móviles Android que deben conectarse con el Servidor de administración. Las notificaciones push se envían entonces a los dispositivos móviles.

11. Dispositivos móviles Android únicamente: las notificaciones push de los servidores de Google se envían al dispositivo móvil. La conexión se utiliza para indicar a los dispositivos móviles que deben conectarse con el Servidor de administración.

12. Dispositivos móviles iOS únicamente: el Servidor de MDM para iOS se comunica con los servidores de notificaciones push de Apple. Las notificaciones push se envían entonces a los dispositivos móviles.

13. Solo para dispositivos móviles iOS: las notificaciones push se envían desde los servidores de Apple al dispositivo móvil. La conexión se utiliza para indicar a los dispositivos móviles iOS que deben conectarse con el Servidor de administración.

14. Dispositivos móviles únicamente: los datos de la aplicación administrada se transfieren al Servidor de administración (o a la puerta de enlace de conexión) a través de los puertos TLS 13292 o 13293, ya sea en forma directa o a través de un proxy inverso.

15. Dispositivos móviles únicamente: datos enviados por el dispositivo móvil a la infraestructura de Kaspersky.

    Si el dispositivo móvil no tiene acceso a Internet, el tráfico se envía primero al Servidor de administración a través del puerto 17100 y el Servidor de administración lo remite a los servidores de Kaspersky. Esta, sin embargo, no es una situación usual.

16. Las solicitudes de paquetes de los dispositivos administrados, incluidos los dispositivos móviles, se transfieren al Servidor web, que se encuentra en el mismo dispositivo que el Servidor de administración.

17. Solo para dispositivos móviles iOS: los datos de los dispositivos móviles se transfieren a través del puerto TLS 443 al servidor de MDM para iOS, que se encuentra en el mismo dispositivo que el Servidor de administración o en la puerta de enlace de conexión.

# Interacción entre los componentes de Kaspersky Security Center y las aplicaciones de seguridad: más información

Esta sección proporciona los esquemas para la interacción de componentes Kaspersky Security Center y aplicaciones de seguridad administradas. Los esquemas proporcionan los números de los puertos que deben estar abiertos y los nombres de los procesos que abren esos puertos.

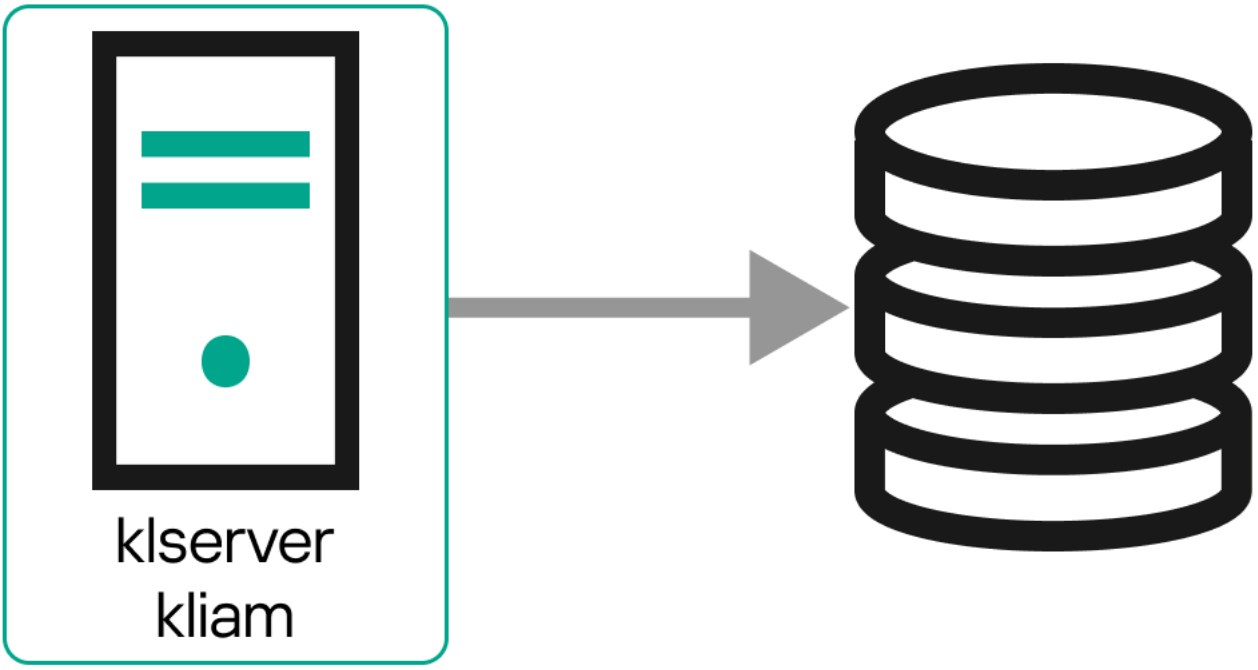
## Convenciones utilizadas en esquemas de interacción

La siguiente tabla proporciona las convenciones usadas en los esquemas.

| Icono | Significado |
|---|---|
|  | Servidor de administración |
|  | Servidor de administración secundario |
|  | DBMS |
|  | El dispositivo cliente (que tiene Agente de red y una aplicación de la familia de Kaspersky Endpoint Security instalada o tiene una aplicación de seguridad diferente instalada que Kaspersky Security Center puede administrar) |
|  | Puerta de enlace de conexión |
|  | Punto de distribución |
|  | Dispositivo cliente móvil que tiene Kaspersky Security for Mobile |
|  | Navegador en el dispositivo del usuario |
|  | Proceso que se ejecuta en el dispositivo y que abre un puerto |
|  | Puerto y su número |
|  | Tráfico de TCP (la dirección de la flecha muestra la dirección del flujo de tráfico) |
|  | Tráfico de UDP (la dirección de la flecha muestra la dirección de flujo del tráfico) |
|  | Invocar COM |
|  | Transporte de DBMS |
|  | Límite de DMZ |

## Servidor de administración y DBMS

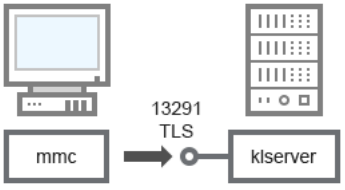
Los datos del Servidor de administración se introducen en la base de datos de SQL Server, MySQL o MariaDB.




Servidor de administración y DBMS

Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo en el que se encuentra la base de datos (por ejemplo, el puerto 3306 para MySQL Server o el puerto 1433 para Microsoft SQL Server). Consulte la documentación del DBMS para obtener la información necesaria.

## Servidor de administración y Consola de administración




Servidor de administración y Consola de administración

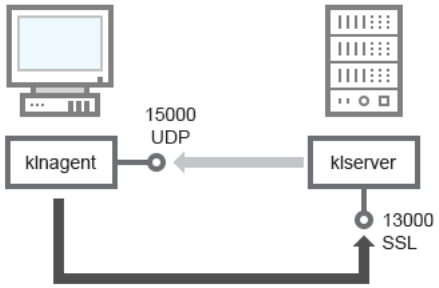
Para aclaraciones del esquema, consulte la tabla a continuación.

Servidor de administración y Consola de administración (tráfico)

| Dispositivo | Número de puerto | Nombre del proceso que abre el puerto | Protocolo | TLS | Objetivo del puerto |
|---|---|---|---|---|---|
| Servidor de administración | 13291 | klserver | TCP | Sí | Recepción de conexiones de la Consola de administración |

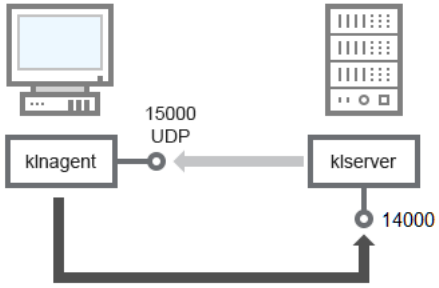
# Servidor de administración y dispositivo cliente: administración de la aplicación de seguridad

El Servidor de administración recibe la conexión de los Agentes de red a través del puerto SSL 13000 (consulte la figura a continuación).




Servidor de administración y dispositivo cliente: administración de la aplicación de seguridad, conexión a través del puerto 13000 (recomendado)

Si usó una versión anterior de Kaspersky Security Center, el Servidor de administración de su red puede recibir conexiones de Agentes de red a través del puerto (no de SSL) 14000 (consulte la figura a continuación). Kaspersky Security Center 15.1 también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto SSL 13000.




Servidor de administración y dispositivo cliente: administración de la aplicación de seguridad, conexión a través del puerto 14000 (menor seguridad)

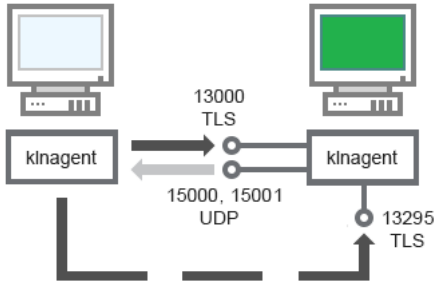
Para explicaciones sobre los esquemas, consulte la tabla a continuación.

Servidor de administración y dispositivo cliente: administración de la aplicación de seguridad (tráfico)

| Dispositivo | Número de puerto | Nombre del proceso que abre el puerto | Protocolo | TLS (solo para TCP) | Objetivo del puerto |
|---|---|---|---|---|---|
| Agente de red | 15000 | klnagent | UDP | Nulo | Multidifusión para Agentes de red |
| Servidor de administración | 13000 | klserver | TCP | Sí | Recepción de conexiones de los agentes de red |
| Servidor de administración | 14000 | klserver | TCP | No | Recepción de conexiones de los agentes de red |

# Actualización de software en un dispositivo cliente a través de un punto de distribución

El dispositivo cliente se conecta al punto de distribución mediante el puerto 13000 y, si utiliza el punto de distribución como servidor push, también mediante el puerto 13295. Se realiza la multidifusión del punto de distribución hacia el Agente de red mediante el puerto 15000 (consulte la imagen siguiente). Las actualizaciones y los paquetes de instalación se reciben desde un punto de distribución a través del puerto 15001.




Actualización de software en un dispositivo cliente a través de un punto de distribución

Para aclaraciones del esquema, consulte la tabla a continuación.

Actualización de software mediante un punto de distribución (tráfico)

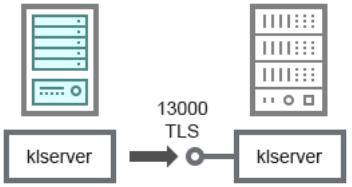
| Dispositivo | Número de puerto | Nombre del proceso que abre el puerto | Protocolo | TLS (solo para TCP) | Objetivo del puerto |
|---|---|---|---|---|---|
| Agente de red | 15000 | klnagent | UDP | Nulo | Multidifusión para Agentes de red |
| Agente de red | 15001 | klnagent | UDP | Nulo | Recepción de actualizaciones y paquetes de instalación de un punto de distribución |
| Punto de distribución | 13000 | klnagent | TCP | Sí | Recepción de conexiones de los agentes de red |
| Punto de distribución | 13295 | klnagent | TCP | Sí | Recepción de conexiones de dispositivos cliente (por el servidor push) |

# Jerarquía de Servidores de administración: Servidor de administración principal y Servidor de administración secundario

El esquema (vea la figura a continuación) muestra cómo usar el puerto 13000 para asegurar la interacción entre los Servidores de administración combinados en una jerarquía.

Al combinar dos Servidores de administración en una jerarquía, asegúrese de que el puerto 13291 esté accesible en ambos Servidores de administración. La Consola de administración se conecta al Servidor de administración a través del puerto 13291.

Posteriormente, cuando los Servidores de administración se combinen en una jerarquía, podrá administrarlos mediante la Consola de administración conectada al Servidor de administración principal. Por lo tanto, la accesibilidad del puerto 13291 del Servidor de administración principal es el único requisito previo.



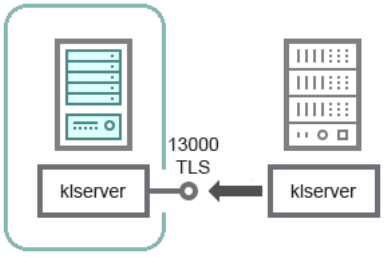

Jerarquía de Servidores de administración: Servidor de administración principal y Servidor de administración secundario

Para aclaraciones del esquema, consulte la tabla a continuación.

Jerarquía de Servidores de administración (tráfico)

| Dispositivo | Número de puerto | Nombre del proceso que abre el puerto | Protocolo | TLS | Objetivo del puerto |
|---|---|---|---|---|---|
| Servidor de administración principal | 13000 | klserver | TCP | Sí | Recepción de conexiones de Servidores de administración secundarios |

# Jerarquía de Servidores de administración con un Servidor de administración secundario en DMZ




Jerarquía de Servidores de administración con un Servidor de administración secundario en DMZ

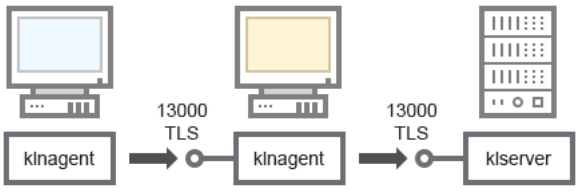
El esquema muestra una jerarquía de Servidores de administración en la que el Servidor de administración secundario ubicado en la "zona desmilitarizada" (DMZ) recibe una conexión del Servidor de administración principal (consulte la tabla a continuación para explicaciones sobre esquemas). Al combinar dos Servidores de administración en una jerarquía, asegúrese de que el puerto 13291 esté accesible en ambos Servidores de administración. La Consola de administración se conecta al Servidor de administración a través del puerto 13291.

Posteriormente, cuando los Servidores de administración se combinen en una jerarquía, podrá administrarlos mediante la Consola de administración conectada al Servidor de administración principal. Por lo tanto, la accesibilidad del puerto 13291 del Servidor de administración principal es el único requisito previo.

Jerarquía de Servidores de administración con un Servidor de administración secundario en DMZ (tráfico)

| Dispositivo | Número de puerto | Nombre del proceso que abre el puerto | Protocolo | TLS | Objetivo del puerto |
|---|---|---|---|---|---|
| Servidor de administración secundario | 13000 | klserver | TCP | Sí | Recepción de conexiones del Servidor de administración principal |

# Servidor de administración, una puerta de enlace de conexión en un segmento de red y un dispositivo cliente



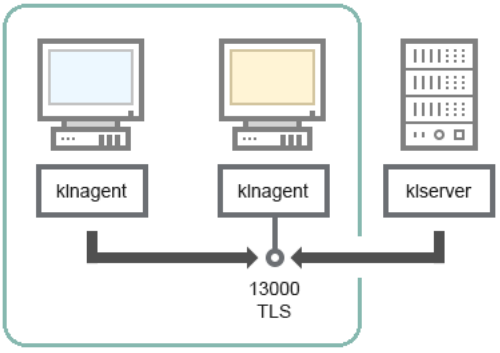

Servidor de administración, una puerta de enlace de conexión en un segmento de red y un dispositivo cliente

Para aclaraciones del esquema, consulte la tabla a continuación.

Servidor de administración con una puerta de enlace de conexión en un segmento de red y un dispositivo cliente (tráfico)

| Dispositivo | Número de puerto | Nombre del proceso que abre el puerto | Protocolo | TLS | Objetivo del puerto |
|---|---|---|---|---|---|
| Servidor de administración | 13000 | klserver | TCP | Sí | Recepción de conexiones de los agentes de red |
| Agente de red | 13000 | klnagent | TCP | Sí | Recepción de conexiones de los agentes de red |

# Servidor de administración y dos dispositivos en DMZ: una puerta de enlace de conexión y un dispositivo cliente



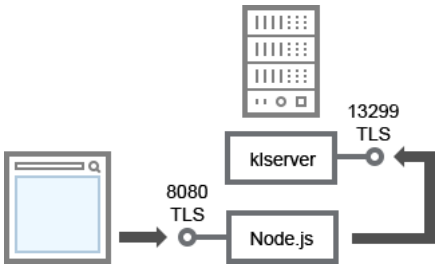

Servidor de administración con una puerta de enlace de conexión y un dispositivo cliente en DMZ

Para aclaraciones del esquema, consulte la tabla a continuación.

Servidor de administración con una puerta de enlace de conexión en un segmento de red y un dispositivo cliente (tráfico)

| Dispositivo | Número de puerto | Nombre del proceso que abre el puerto | Protocolo | TLS | Objetivo del puerto |
|---|---|---|---|---|---|
| Agente de red | 13000 | klnagent | TCP | Sí | Recepción de conexiones de los agentes de red |

# Servidor de administración y Kaspersky Security Center Web Console




Servidor de administración y Kaspersky Security Center Web Console

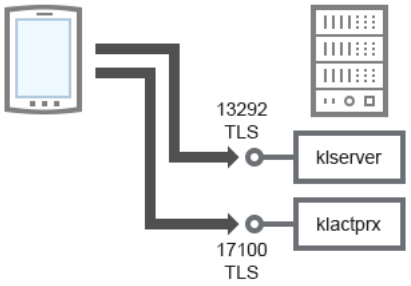
Para aclaraciones del esquema, consulte la tabla a continuación.

Servidor de administración y Kaspersky Security Center Web Console (tráfico)

| Dispositivo | Número de puerto | Nombre del proceso que abre el puerto | Protocolo | TLS | Objetivo del puerto |
|---|---|---|---|---|---|
| Servidor de administración | 13299 | klserver | TCP | Sí | Recepción de conexiones desde Kaspersky Security Center Web Console al Servidor de administración a través de OpenAPI |
| Servidor de administración o Servidor de Kaspersky Security Center Web Console | 8080 | Node.js: JavaScript del lado del servidor | TCP | Sí | Recibiendo conexiones de Kaspersky Security Center Web Console |

Kaspersky Security Center Web Console se puede instalar en el Servidor de administración o en otro dispositivo.

# Activación y administración de la aplicación de seguridad en un dispositivo móvil




Activación y administración de la aplicación de seguridad en un dispositivo móvil

Para aclaraciones del esquema, consulte la tabla a continuación.

Activación y administración de la aplicación de seguridad en un dispositivo móvil (tráfico)

| Dispositivo | Número de puerto | Nombre del proceso que abre el puerto | Protocolo | TLS | Objetivo del puerto |
|---|---|---|---|---|---|
| Servidor de administración | 13292 | klserver | TCP | Sí | Recepción de conexiones de la Consola de administración destinadas al Servidor de administración |
| Servidor de administración | 17100 | klactprx | TCP | Sí | Recepción de conexiones para la activación de la aplicación de dispositivos móviles |

# Prácticas recomendadas para el despliegue

Kaspersky Security Center es una aplicación distribuida. Kaspersky Security Center incluye las aplicaciones siguientes:

- Servidor de administración: El componente principal, diseñado para administrar los dispositivos de una organización y almacenar datos en un DBMS.
- Consola de administración: La herramienta básica para el administrador. La Consola de administración se envía junto con el Servidor de administración, pero también se puede instalar individualmente en uno o varios dispositivos ejecutados por el administrador.
- Agente de red: Diseñado para administrar la aplicación de seguridad instalada en un dispositivo, así como para recopilar información sobre ese dispositivo y transferir esta información al Servidor de administración. Los agentes de red se instalan en dispositivos de una organización.

El despliegue de Kaspersky Security Center en la red de una organización se realiza de la siguiente manera:

- Instalación de un Servidor de administración.
- Instalación de la Consola de administración en el dispositivo del administrador.
- Instalación del Agente de red y aplicación de seguridad en dispositivos de la empresa.

# Guía para reforzar la seguridad

Kaspersky Security Center está diseñado para ejecutar tareas de administración y mantenimiento básicas en la red de una organización de forma centralizada. La aplicación proporciona al administrador acceso a información detallada sobre el nivel de seguridad de la red de la organización. Kaspersky Security Center le permite configurar todos los componentes de protección creados con las aplicaciones de Kaspersky.

El Servidor de administración de Kaspersky Security Center tiene acceso completo a la administración de protección de los dispositivos cliente y es el componente más importante del sistema de seguridad de la organización. Por lo tanto, se requieren métodos de mayor protección para el Servidor de administración.

Antes de la configuración, cree una copia de seguridad del Servidor de administración de Kaspersky Security Center con la tarea Copia de seguridad de los datos del Servidor de administración o la utilidad klbackup y guárdela en un lugar seguro.

La Guía para reforzar la seguridad describe recomendaciones y funciones para configurar Kaspersky Security Center y sus componentes, con el objetivo de reducir los riesgos de compromiso.

La Guía para reforzar la seguridad contiene la siguiente información:

- Selección de la arquitectura del Servidor de administración
- Configuración de una conexión segura al Servidor de administración
- Configuración de las cuentas para acceder al Servidor de administración

- Administrar la protección del Servidor de administración
- Administración de la protección de dispositivos cliente
- Configurar la protección para aplicaciones administradas
- Mantenimiento del Servidor de administración
- Transferencia de información a aplicaciones de terceros
- Recomendaciones de seguridad para sistemas de información de terceros

# Instalación del Servidor de administración

## Arquitectura del Servidor de administración

En general, la elección de una arquitectura de administración centralizada depende de la ubicación de los dispositivos protegidos, el acceso desde redes adyacentes, los esquemas de entrega de actualizaciones de bases de datos, etc.

En la etapa inicial del desarrollo de la arquitectura, recomendamos familiarizarse con los componentes de Kaspersky Security Center y su interacción entre sí, así como con esquemas de tráfico de datos y uso de puertos.

Basándose en esta información, puede formar una arquitectura que especifique:

- la ubicación del Servidor de administración y las conexiones de red.
- la organización de los espacios de trabajo del administrador y los métodos de conexión al Servidor de administración.
- métodos de despliegue del Agente de red y el software de protección.
- el uso de puntos de distribución.
- el uso de Servidores de administración virtuales.
- usar una jerarquía de Servidores de administración.
- esquema de actualización de la base de datos antivirus.
- otros flujos de información.

## la selección de un dispositivo para la instalación del Servidor de administración.

Recomendamos instalar el Servidor de administración en un servidor dedicado en la infraestructura de la organización. Si no hay otro software de terceros instalado en el servidor, puede configurar los ajustes de seguridad según los requisitos de Kaspersky Security Center, sin depender de los requisitos del software de terceros.

Puede desplegar el Servidor de administración en un servidor físico o en un servidor virtual. Asegúrese de que el dispositivo seleccionado cumple los requisitos de hardware y software.

## Ubicación del Servidor de administración

Los dispositivos administrados por el Servidor de administración se pueden ubicar de la siguiente manera:

- En una red de área local (LAN)
- En Internet
- En la zona desmilitarizada (DMZ)

Al mismo tiempo, el Servidor de administración también se puede ubicar en diferentes segmentos: industrial, corporativo y DMZ.

Si usa Kaspersky Security Center para administrar la protección de un segmento de red aislado, le recomendamos desplegar el Servidor de administración en un segmento de la zona desmilitarizada (DMZ). Esto le permite organizar una segmentación de red adecuada y minimizar el flujo de tráfico al segmento protegido, mientras se mantienen las capacidades de administración completas y la entrega de actualizaciones.

## Restricción de despliegue del Servidor de administración en un controlador de dominio, un servidor de terminal o un dispositivo de usuario

Desaconsejamos instalar el Servidor de administración en un controlador de dominio, un servidor de terminales o un dispositivo de usuario.

Le recomendamos que proporcione una separación funcional de los nodos clave de la red. Este enfoque le permite mantener la operatividad de diferentes sistemas cuando un nodo falla o se ve comprometido. Al mismo tiempo, puede crear diferentes políticas de seguridad para cada nodo.

Por ejemplo, las restricciones de seguridad que normalmente se aplican a un controlador de dominio pueden reducir significativamente el rendimiento del Servidor de administración e imposibilitar el uso de algunas de las funciones del Servidor de administración. Si un intruso obtiene acceso privilegiado al controlador de dominio, la base de datos de Servicios de dominio de Active Directory (AD DS) puede resultar modificada, dañada o destruida. Además, todos los sistemas y cuentas administrados por Active Directory pueden verse comprometidos.

## Cuentas para instalar y ejecutar el Servidor de administración

Recomendamos ejecutar la instalación del Servidor de administración con una cuenta de administrador local para evitar el uso de cuentas de dominio para acceder a la base de datos del Servidor de administración. Un conjunto de cuentas requeridas y sus derechos depende del tipo de DBMS seleccionado, la ubicación del DBMS y el método de creación de la base de datos del Servidor de administración.

Los grupos KLAdmins y KLOperators se crean automáticamente durante la instalación de Kaspersky Security Center. A estos grupos se les otorgan permisos para conectarse al Servidor de administración y procesar los objetos de este.

Según el tipo de cuenta que se use para instalar Kaspersky Security Center, los grupos KLAdmins y KLOperators se crean de la siguiente manera:

- Si la aplicación se instala con una cuenta de usuario incluida en un dominio, los grupos se crean en el dispositivo Servidor de administración y en el dominio que incluye el Servidor de administración.
- Si la aplicación se instala con una cuenta de sistema, los grupos se crean solo en el dispositivo Servidor de administración.

Para evitar crear los grupos KLAdmins y KLOperators en el dominio y, como resultado, **proporcionar privilegios para administrar el Servidor de administración a una cuenta fuera del dispositivo del Servidor de administración**, recomendamos instalar Kaspersky Security Center con una cuenta local.

Durante la instalación del Servidor de administración, seleccione la cuenta que se utilizará para iniciar el Servidor de administración como servicio. De manera predeterminada, la aplicación crea una cuenta local llamada KL-AK-*, en la que se ejecutará el servicio del Servidor de administración (el servicio klserver).

Si es necesario, el servicio del Servidor de administración se puede ejecutar con la cuenta seleccionada. Esta cuenta debe tener los derechos necesarios para acceder al DBMS. Por motivos de seguridad, utilice una cuenta sin privilegios para ejecutar el servicio del Servidor de administración.

Para evitar el uso de configuraciones de cuenta incorrectas, le recomendamos generar la cuenta automáticamente.

### Exclusión del Servidor de administración de un dominio

Si usa el Servidor de administración para proteger grupos de dispositivos de sistemas de gran importancia, no recomendamos incluir el dispositivo del Servidor de administración en el dominio. Esto le permite diferenciar los derechos de administración de Kaspersky Security Center y evitar el acceso al Servidor de administración en caso de que la cuenta de dominio se vea comprometida.

Tenga en cuenta que, si instala el Servidor de administración en un dispositivo incluido en el grupo de trabajo, los siguientes escenarios de trabajo con el Servidor de administración no estarán disponibles:

- Uso de un clúster de conmutación por error de Kaspersky Security Center
- Uso de un clúster de conmutación por error de Windows Server
- Uso de SQL Server para Windows en un dispositivo separado

  Puede usar SQL Server para Windows en un dispositivo separado solo si el Servidor de administración y SQL Server están en el mismo dominio o en dominios de confianza. Si el Servidor de administración, SQL Server y un recurso compartido de UNC para copias de seguridad están en un grupo de trabajo, no puede configurar de forma segura los derechos de acceso y lectura y escritura entre SQL Server y el recurso compartido.
- Instalación remota con herramientas del Servidor de administración a través de directivas de grupo de Active Directory

Si necesita desconectar el Servidor de administración del dominio de Active Directory, siga los pasos descritos en el tema: Cómo cambiar el nombre de Kaspersky Security Center.

Si es necesario instalar el Servidor de administración en un dispositivo incluido en el grupo de trabajo, puede usar Kaspersky Security Center Linux en lugar de Kaspersky Security Center Windows.

## Seguridad de la conexión

### Uso de TLS

Recomendamos prohibir las conexiones no seguras al Servidor de administración. Por ejemplo, puede prohibir las conexiones que usan HTTP en la configuración del Servidor de administración.

Tenga en cuenta que, de forma predeterminada, varios puertos HTTP del Servidor de administración están cerrados. El puerto restante se utiliza para el servidor web del Servidor de administración (8060). Este puerto puede estar limitado por la configuración del firewall del dispositivo del Servidor de Administración.

## Configuración estricta de TLS

Le recomendamos usar el protocolo TLS de la versión 1.2 y posteriores, y restringir o prohibir los algoritmos de cifrado inseguros.

Puede configurar los protocolos de cifrado (TLS) usados por el Servidor de administración. Tenga en cuenta que, en el momento de lanzar una versión del Servidor de administración, la configuración del protocolo de cifrado está configurada de forma predeterminada para garantizar una transferencia de datos segura.

## Prohibición de autenticación remota mediante el uso de cuentas de Windows

Puede usar el indicador LP_RestrictRemoteOsAuth para prohibir las conexiones SSPI desde direcciones remotas. Este indicador le permite prohibir la autenticación remota en el Servidor de administración mediante el uso de cuentas de Windows locales o de dominio.

*Para cambiar el indicador LP_RestrictRemoteOsAuth al modo de prohibición de conexiones desde las direcciones remotas:*

1. Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada es <Disk>:\Archivos de programa(x86)\Kaspersky Lab\Kaspersky Security Center.

2. Ejecute el siguiente comando en la línea de comandos para especificar el valor del indicador LP_RestrictRemoteOsAuth:

   ```
   klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_RestrictRemoteOsAuth -t d -v 1
   ```

3. Reinicie el servicio del Servidor de administración.

El indicador LP_RestrictRemoteOsAuth no funciona si la autenticación remota se realiza a través de Kaspersky Security Center Web Console o la Consola de administración que está instalada en el dispositivo del Servidor de administración.

## Restricción del acceso a la base de datos del Servidor de administración

Recomendamos restringir el acceso a la base de datos del Servidor de administración. Por ejemplo, conceda el acceso solo desde el dispositivo del Servidor de administración. Esto reduce la probabilidad de que la base de datos del Servidor de administración se vea comprometida debido a vulnerabilidades conocidas.

Puede configurar los parámetros de acuerdo con las instrucciones de funcionamiento de la base de datos usada, así como proporcionar puertos cerrados en los firewalls.

## Autenticación de Microsoft SQL Server

Si Kaspersky Security Center usa Microsoft SQL Server como DBMS, es necesario proteger los datos de Kaspersky Security Center transferidos hacia o desde la base de datos y los datos almacenados en la base de datos del acceso no autorizado. Para hacer esto, debe proporcionar una comunicación segura entre Kaspersky Security Center y SQL Server. La forma más confiable de garantizar una comunicación segura es instalar Kaspersky Security Center y SQL Server en el mismo dispositivo y usar el mecanismo de memoria compartida para ambas aplicaciones. En los demás casos, le recomendamos que use un certificado SSL o TLS para autenticar la instancia de SQL Server.

Por lo general, el Servidor de administración puede dirigirse a SQL Server a través de los siguientes proveedores:

- SQLOLEDB mediante TCP/IP o canalizaciones con nombre

  Este proveedor se instala en el sistema operativo Windows y se utiliza de manera predeterminada.

- MSOLEDBSQL mediante TCP/IP, canalizaciones con nombre o memoria compartida

  Si desea utilizar este proveedor, debe instalarlo en el dispositivo con el Servidor de administración y, luego, establecer el valor `1` en la variable de entorno global `KLDBADO_UseMSOLEDBSQL`.

- MSOLEDBSQL mediante TCP/IP, canalizaciones con nombre o memoria compartida

  Si desea utilizar este proveedor, debe instalarlo en el dispositivo con el Servidor de administración y luego establecer el valor `1` en la variable de entorno global `KLDBADO_UseMSOLEDBSQL` y el valor `MSOLEDBSQL19` en la variable de entorno global `KLDBADO_ProviderName`.

Además, antes de usar TCP/IP, canalizaciones con nombre o memoria compartida, asegúrese de que el protocolo requerido esté habilitado.

## Interacción de seguridad con un SGBD externo

Si el SGBD se instala en un dispositivo independiente durante la instalación del Servidor de Administración (SGBD externo), recomendamos configurar los parámetros para una interacción y autenticación seguras con este SGBD. Para obtener más información sobre cómo configurar la autenticación SSL, consulte Autenticación del servidor PostgreSQL y Escenario: autenticación del servidor MySQL.

## Configuración de una lista de admitidos de direcciones IP para conectarse al Servidor de administración

De forma predeterminada, los usuarios de Kaspersky Security Center pueden iniciar sesión en Kaspersky Security Center desde cualquier dispositivo donde estén instaladas la Consola de administración basada en MMC, Kaspersky Security Center Web Console o las aplicaciones OpenAPI. Puede hacer que el Servidor de administración únicamente acepte conexiones de dispositivos que tengan una dirección IP permitida. Por ejemplo, si un intruso intenta conectarse a Kaspersky Security Center a través del Servidor de Kaspersky Security Center Web Console instalado en un dispositivo que no está incluido en la lista de admitidos, no podrá iniciar sesión en Kaspersky Security Center.

### Configurar una lista de direcciones IP permitidas para conectarse con Kaspersky Security Center Web Console

De manera predeterminada, los usuarios de Kaspersky Security Center pueden conectarse a Kaspersky Security Center Web Console desde cualquier dispositivo. En un dispositivo con Kaspersky Security Center Web Console instalado, debe configurar el firewall (integrado en el sistema operativo o en uno de terceros) para que los usuarios puedan conectarse a Kaspersky Security Center Web Console solo desde las direcciones IP permitidas.

### Seguridad de la conexión al controlador de dominio durante el sondeo

El Servidor de administración o un punto de distribución de Linux se conectan al controlador de dominio a través de LDAPS para sondear el dominio. De forma predeterminada, la verificación del certificado no es obligatoria al conectarse. Para hacer verificar el certificado, establezca el indicador `KLNAG_LDAP_TLS_REQCERT` en 1. Además, puede especificar una ruta personalizada a la autoridad de certificación (CA) para acceder a la cadena de certificados utilizando el indicador `KLNAG_LDAP_SSL_CACERT`.

## Cuentas y autenticación

Antes de realizar los siguientes pasos, cree una copia de seguridad del Servidor de administración de Kaspersky Security Center con la tarea Copia de seguridad de los datos del Servidor de administración o con la utilidad klbackup y guárdela en un lugar seguro.

### Uso de la verificación en dos pasos con el Servidor de administración

**Kaspersky Security Center proporciona verificación en dos pasos** para usuarios de Kaspersky Security Center Web Console y la Consola de administración, según el estándar RFC 6238 (TOTP: algoritmo de contraseña de un solo uso basado en tiempo).

Cuando la verificación en dos pasos está activada para su propia cuenta, cada vez que inicie sesión en Kaspersky Security Center Web Console o la Consola de administración, debe introducir su nombre de usuario, contraseña y un código de seguridad adicional de un solo uso. Si utiliza la autenticación de dominio para su cuenta, solo tiene que ingresar un código de seguridad adicional de un solo uso. Para recibir un código de seguridad de un solo uso, debe haber instalado una app de autenticación en su computadora o dispositivo móvil.

Existen autenticadores de software y de hardware (tokens) que admiten el estándar RFC 6238. Por ejemplo, los autenticadores de software incluyen Google Authenticator, Microsoft Authenticator o FreeOTP.

No recomendamos en absoluto instalar la app de autenticación en el mismo dispositivo desde el que se establece la conexión con el Servidor de administración. Puede instalar una app de autenticación en su dispositivo móvil.

#### Prohibir a los nuevos usuarios configurar la verificación en dos pasos por sí mismos

Para mejorar aún más la seguridad del acceso a Kaspersky Security Center Web Console, puede prohibir a los nuevos usuarios configurar ellos mismos la verificación en dos pasos.

Si esta opción está habilitada, un usuario con la verificación en dos pasos deshabilitada, por ejemplo, un nuevo administrador de dominio, no puede configurar la verificación en dos pasos por sí mismo. Por lo tanto, dicho usuario no puede autenticarse en el Servidor de administración y no puede iniciar sesión en Kaspersky Security Center Web Console sin la aprobación de otro administrador de Kaspersky Security Center que ya tenga activada la verificación en dos pasos.

## Uso de la autenticación de dos factores para un sistema operativo

Recomendamos utilizar la autenticación multifactor (MFA) para la autenticación en el dispositivo del Servidor de administración mediante un token, una tarjeta inteligente u otro método (si es posible).

## Restringir el guardado de la contraseña de administrador

Si utiliza la Consola de administración, no recomendamos guardar la contraseña de administrador en el cuadro de diálogo de conexión del Servidor de administración.

Si utiliza Kaspersky Security Center Web Console, no recomendamos guardar la contraseña de administrador en el navegador instalado en el dispositivo del usuario.

## Autenticación de una cuenta de usuario interna

Por defecto, la contraseña de una cuenta de usuario interna del Servidor de Administración debe cumplir con las siguientes reglas:

- La contraseña debe tener entre 8 y 256 caracteres.
- La contraseña debe incluir caracteres de al menos tres de los grupos enumerados a continuación:
  - Letras mayúsculas (A-Z)
  - Letras minúsculas (a-z)
  - Números (0-9)
  - Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- La contraseña no debe contener espacios en blanco, caracteres Unicode o la combinación de "." y "@" cuando "." está colocado delante de "@".

De forma predeterminada, el número máximo de intentos permitidos para introducir una contraseña es 10. Puede cambiar el número de intentos de entrada de contraseña permitidos.

El usuario de Kaspersky Security Center puede introducir una contraseña no válida un número limitado de veces. Una vez que se alcanza el límite, la cuenta de usuario se bloquea durante una hora.

## Configurar las opciones para cambiar la contraseña de una cuenta de usuario interno

Recomendamos configurar las siguientes opciones para cambiar la contraseña de una cuenta de usuario interno:

- Período de rotación de contraseñas
- Tiempo de la advertencia preliminar sobre la necesidad de cambiar la contraseña
- Valor de la opción **El usuario debe cambiar la contraseña la primera vez que inicie sesión**

## Protección de una cuenta contra modificaciones sin autorización

Recomendamos habilitar una opción adicional para proteger una cuenta de usuario interno del Servidor de administración contra modificaciones no autorizadas. Esta protección debe configurarse por separado para cada usuario interno.

## Grupo de administración dedicado para el Servidor de administración

Recomendamos crear un grupo de administración dedicado para el Servidor de administración. Otorgue a este grupo derechos de acceso especiales y cree una directiva de seguridad especial para él.

Para evitar bajar intencionadamente el nivel de seguridad del Servidor de administración, recomendamos restringir la lista de cuentas que puede administrar el grupo de administración dedicado.

## Los grupos KLAdmins y KLOperators

Los grupos KLAdmins y KLOperators se crean automáticamente durante la instalación de Kaspersky Security Center. El grupo KLAdmins tiene todos los derechos de acceso. El grupo KLOperators solo tiene derechos de lectura y ejecución. Los permisos otorgados al grupo KLAdmins están **bloqueados**.

Puede ver los grupos KLAdmins y KLOperators, y realizar cambios en estos grupos, mediante las herramientas administrativas estándar del sistema operativo.

Al desarrollar regulaciones para trabajar con el Servidor de administración, es necesario determinar si el especialista en seguridad de la información necesita acceso completo (e inclusión en el grupo KLAdmins) para realizar tareas estándar.

La mayoría de las tareas básicas de administración se pueden distribuir entre departamentos de la empresa (o diferentes empleados del mismo departamento) y, en consecuencia, entre diferentes cuentas. También puede configurar la diferenciación de acceso a los grupos de administración en Kaspersky Security Center. Como resultado, es posible implementar un escenario en el que la autorización en las cuentas del grupo KLAdmins será anómala y podría considerarse un incidente.

Si Kaspersky Security Center se instaló en una cuenta del sistema, solo se crean grupos en el dispositivo del Servidor de administración. En este caso, recomendamos asegurarse de que solo se incluyan en el grupo las entradas creadas durante la instalación de Kaspersky Security Center. No recomendamos agregar ningún grupo al grupo KLAdmins (local o dominio) que se crea automáticamente durante la instalación de Kaspersky Security Center. También debe limitar los derechos para cambiar este grupo. El grupo KLAdmins debe incluir solo cuentas individuales sin privilegios.

Si la instalación se realizó con una cuenta de usuario de dominio, los grupos KLAdmins y KLOperators se crean tanto en el Servidor de administración como en el dominio que incluye el Servidor de administración. Se recomienda un enfoque similar, como la instalación de una cuenta local.

## Restricción de la pertenencia a la función de Administrador principal

Recomendamos restringir la pertenencia al rol de Administrador principal.

De forma predeterminada, después de la instalación del Servidor de administración, la función de Administrador principal se asigna al grupo de administradores locales y al grupo KLAdmins creado. Es útil para la administración, pero es crítico desde el punto de vista de la seguridad; debido a que el rol de Administrador Principal tiene una amplia gama de privilegios, la asignación de este rol a los usuarios debe estar estrictamente regulada.

Los administradores locales se pueden excluir de la lista de usuarios con privilegios de administrador de Kaspersky Security Center. La función de administrador principal no se puede eliminar del grupo KLAdmins. Puede incluir en el grupo KLAdmins las cuentas que se usarán para administrar el Servidor de administración.

Si utiliza la autenticación de dominio, le recomendamos que restrinja los privilegios de las cuentas de administrador de dominio en Kaspersky Security Center. De forma predeterminada, estas cuentas tienen la función de administrador principal. Además, un administrador de dominio puede incluir su cuenta en el grupo KLAdmins para obtener la función de Administrador principal. Para evitarlo, en la configuración de seguridad de Kaspersky Security Center, puede agregar el grupo Administradores de dominio y luego definir reglas de prohibición para él. Estas reglas deben prevalecer sobre las reglas de permisos.

También puede utilizar las funciones de usuario predefinidas con un conjunto de derechos ya configurado.

## Configurar los derechos de acceso a las funciones de la aplicación

Recomendamos utilizar una configuración flexible de los derechos de acceso a las funciones de Kaspersky Security Center para cada usuario o grupo de usuarios.

El control de acceso basado en funciones permite la creación de funciones de usuario estándar con un conjunto de derechos preestablecido y la asignación de esas funciones a los usuarios según su ámbito de responsabilidad.

Las principales ventajas del modelo de control de acceso basado en funciones:

- Facilidad de administración
- Jerarquía de funciones
- Enfoque de privilegios mínimos
- Segregación de deberes

Puede asignar funciones integradas a ciertos empleados en función de sus puestos o crear funciones completamente nuevas.

Al configurar funciones, preste atención a los privilegios asociados con el cambio del estado de protección del dispositivo del Servidor de administración y la instalación remota de software de terceros:

- Administrar grupos de administración.
- Operaciones con el Servidor de administración.

- Instalación remota.
- Cambiar los parámetros para almacenar eventos y enviar notificaciones.

  Este privilegio le permite configurar notificaciones que ejecutan un script o un módulo ejecutable en el dispositivo del Servidor de administración cuando ocurra un evento.

### Cuenta separada para la instalación remota de aplicaciones

Además de la diferenciación básica de derechos de acceso, recomendamos restringir la instalación remota de aplicaciones para todas las cuentas (excepto para el Administrador principal u otra cuenta especializada).

Recomendamos usar una cuenta aparte para la instalación remota de aplicaciones. Puede asignar un rol o permisos a la cuenta separada.

### Asegurar el acceso privilegiado de Windows

Recomendamos tener en cuenta las recomendaciones de Microsoft para proporcionar seguridad de acceso privilegiado. Para ver estas recomendaciones, consulte el artículo Protección del acceso con privilegios.

Uno de los puntos clave de las recomendaciones es la implementación de estaciones de trabajo con acceso con privilegios (PAW).

### Usar una cuenta de servicios administrados (MSA) o cuentas de servicios administrados en grupo (gMSA) para ejecutar el servicio del Servidor de administración

Active Directory tiene un tipo especial de cuentas para ejecutar servicios de forma segura, llamado cuenta de servicios administrados en grupo (MSA/gMSA). Kaspersky Security Center es compatible con cuentas de servicios administrados (MSA) y cuentas de servicios administrados en grupo (gMSA). Si se utilizan estos tipos de cuentas en su dominio, puede seleccionar una de ellas como la cuenta para el servicio del Servidor de administración.

### Auditoría periódica de todos los usuarios y las acciones de los usuarios

Recomendamos realizar una auditoría regular de todos los usuarios en el dispositivo del Servidor de administración. Esto le permite responder a ciertos tipos de amenazas de seguridad asociadas con un posible compromiso del dispositivo.

Además, puede realizar un seguimiento de las acciones de los usuarios, como conectarse y desconectarse del Servidor de administración, conectarse al Servidor de administración con un error y modificar los objetos (para los objetos que admiten la administración de revisiones).

## Administrar la protección del Servidor de administración

### Selección de un software de protección del Servidor de administración

Según el tipo de instalación del Servidor de administración y la estrategia de protección general, seleccione la aplicación para proteger el dispositivo del Servidor de administración.

Si despliega el Servidor de administración en un dispositivo dedicado, le recomendamos que seleccione la aplicación Kaspersky Endpoint Security para proteger el dispositivo del Servidor de administración. Esto permite aplicar todas las tecnologías disponibles para proteger el dispositivo del Servidor de administración, incluidos los módulos de análisis de comportamiento.

Si el Servidor de administración está instalado en un dispositivo que existe en la infraestructura y se ha utilizado previamente para otras tareas, recomendamos considerar el siguiente software de protección:

- Kaspersky Industrial CyberSecurity for Nodes. Recomendamos instalar esta aplicación en dispositivos que estén incluidos en una red industrial. Kaspersky Industrial CyberSecurity for Nodes es una aplicación que cuenta con certificados de compatibilidad con varios fabricantes de software industrial.

- Soluciones de seguridad recomendadas. Si el Servidor de administración está instalado en un dispositivo junto con otras aplicaciones, tenga en cuenta las recomendaciones de quienes hayan desarrollado ese software en cuanto a su compatibilidad con diferentes soluciones de seguridad (puede que ya haya recomendaciones para elegir una solución de seguridad y que deba configurar la zona de confianza).

## Creación de una directiva de seguridad independiente para la aplicación de protección

Recomendamos crear una directiva de seguridad independiente para la aplicación que protege el dispositivo del Servidor de administración. Esta directiva debe ser diferente de la política de seguridad para dispositivos cliente. Esto permite especificar la configuración de seguridad más adecuada para el Servidor de administración, sin afectar el nivel de protección de otros dispositivos.

Recomendamos dividir los dispositivos en grupos y luego colocar el dispositivo del Servidor de administración en un grupo separado, para el cual puede crear una directiva de seguridad especial.

## Módulos de protección

Si no hay recomendaciones especiales del proveedor del software de terceros instalado en el mismo dispositivo que el Servidor de administración, recomendamos activar y configurar todos los módulos de protección disponibles (tras comprobar el funcionamiento de los mismos durante un tiempo determinado).

## Configuración del firewall del dispositivo del Servidor de administración

En el dispositivo del Servidor de administración, recomendamos configurar el firewall para restringir el número de dispositivos que los administradores pueden conectar al Servidor de administración a través de la Consola de administración o Kaspersky Security Center Web Console.

De forma predeterminada, el Servidor de administración usa el puerto 13291 para recibir conexiones desde la Consola de administración, y el puerto 13299 para recibir conexiones desde la Kaspersky Security Center Web Console. Recomendamos restringir la cantidad de dispositivos desde los que se puede administrar el Servidor de administración mediante el uso de estos puertos.

# Administración de la protección de dispositivos cliente

## Restricción al agregar claves de licencia a paquetes de instalación

Los paquetes de instalación se almacenan en la carpeta compartida del Servidor de administración, en la subcarpeta Paquetes. Si agrega una clave de licencia a un paquete de instalación, la clave de licencia puede verse comprometida porque los derechos de acceso de lectura compartidos están activados para el repositorio de paquetes de instalación.

Para no poner en riesgo la clave de licencia, no recomendamos agregar claves de licencia a los paquetes de instalación.

Recomendamos usar la distribución automática de claves de licencia a los dispositivos administrados, el despliegue al ejecutar la tarea de agregar una clave de licencia a una aplicación administrada, y agregar manualmente un código de activación o un archivo clave a los dispositivos.

## Reglas automáticas para trasladar dispositivos automáticamente entre los grupos de administración

Recomendamos restringir el uso de reglas automáticas para mover dispositivos entre grupos de administración.

Si usa reglas automáticas para mover dispositivos, puede conducir a la propagación de directivas que otorguen más privilegios al dispositivo movido que los que tenía antes de la reubicación.

Además, mover un dispositivo cliente a otro grupo de administración puede provocar la propagación de la configuración de políticas. Estas configuraciones de políticas pueden ser indeseables para su distribución a dispositivos invitados y no confiables.

Esta recomendación no se aplica a la asignación inicial única de dispositivos a grupos de administración.

## Requisitos de seguridad para puntos de distribución y puertas de enlace de conexión

Los dispositivos con Network Agent instalado pueden actuar como punto de distribución y realizar las siguientes funciones:

- Distribuir actualizaciones y paquetes de instalación recibidos del Servidor de administración a los dispositivos cliente dentro del grupo.
- Realizar la instalación remota de software de terceros y aplicaciones de Kaspersky en dispositivos cliente.
- Sondear la red para detectar nuevos dispositivos y actualizar la información disponible sobre los dispositivos de los que ya se tenía conocimiento. El punto de distribución puede utilizar los mismos métodos de detección de dispositivos que el Servidor de administración.

Colocar puntos de distribución en la red de la organización que se utilizan para:

- reducir la carga del Servidor de administración
- optimizar el tráfico
- proporcionar al Servidor de administración acceso a dispositivos en puntos poco accesibles de la red de la organización

Teniendo en cuenta las capacidades disponibles, recomendamos proteger los dispositivos que actúan como puntos de distribución de cualquier tipo de acceso no autorizado (incluido el físico).

## Restricción de la asignación automática de los puntos de distribución

Para simplificar la administración y mantener la operatividad de la red, recomendamos utilizar la asignación automática de puntos de distribución. Sin embargo, para redes industriales y redes pequeñas, le recomendamos que no asigne puntos de distribución automáticamente, ya que, por ejemplo, la información privada de las cuentas utilizadas para forzar tareas de instalación remota, puede transferirse a puntos de distribución por medio del sistema operativo.

Para redes industriales y redes pequeñas, puede asignar dispositivos manualmente para que actúen como puntos de distribución.

También puede ver el Informe de actividad de puntos de distribución.

## Requisitos de seguridad para los dispositivos de los usuarios de Kaspersky Security Center

Se deben aplicar requisitos de seguridad especiales a los dispositivos de los usuarios de Kaspersky Security Center. Recomendamos proteger estos dispositivos contra cualquier tipo de acceso no autorizado (incluso físicamente):

Los dispositivos de usuario de Kaspersky Security Center incluyen los siguientes:

- Dispositivos desde los cuales los usuarios se conectan a Kaspersky Security Center Web Console mediante un navegador.
- Dispositivos desde los cuales los usuarios se conectan a Kaspersky Security Center mediante la Consola de administración basada en MMC.
- Dispositivos desde los cuales las aplicaciones que interactúan con el Servidor de administración a través de OpenAPI están conectadas a Kaspersky Security Center.

## Requisitos de seguridad para dispositivos con Kaspersky Security Center Web Console instalado

Los dispositivos con Kaspersky Security Center Web Console instalado se utilizan para administrar Kaspersky Security Center, por lo que deben aplicarse requisitos especiales a la seguridad de estos dispositivos. Recomendamos proteger estos dispositivos contra cualquier tipo de acceso no autorizado (incluso físicamente).

# Configurar la protección para aplicaciones administradas

## Políticas de aplicaciones administradas

Recomendamos crear una directiva para cada tipo de aplicación y componente de Kaspersky Security Center que se utilice (Agente de red, Kaspersky Endpoint Security para Windows, Kaspersky Endpoint Agent y otros). Esta directiva debe aplicarse a todos los dispositivos administrados (el grupo de administración raíz) o a un grupo aparte al que se mueven automáticamente los nuevos dispositivos administrados de acuerdo con las reglas de movimiento configuradas.

## Especificar la contraseña para desactivar la protección y desinstalar la aplicación

**Para evitar que los intrusos deshabiliten las aplicaciones de seguridad de Kaspersky, recomendamos encarecidamente habilitar la protección con contraseña para deshabilitar la protección y la desinstalación de las aplicaciones de seguridad de Kaspersky.** Puede configurar la contraseña, por ejemplo, para Kaspersky Endpoint Security para Windows, Kaspersky Security for Windows Server, Agente de red y otras aplicaciones de Kaspersky. Después de habilitar la protección con contraseña, recomendamos bloquear esta configuración cerrando el "candado".

## Especificación de la contraseña para la conexión manual de un dispositivo cliente al Servidor de administración (utilidad klmover)

La utilidad klmover le permite conectar manualmente un dispositivo cliente al Servidor de administración. Al instalar el Agente de red en un dispositivo cliente, la utilidad se copia automáticamente a la carpeta de instalación del Agente de red.

Para evitar que los intrusos muevan los dispositivos fuera del control de su Servidor de administración, recomendamos que active la protección con contraseña para ejecutar la utilidad klmover. Para habilitar la protección con contraseña, seleccione la opción **Utilizar contraseña de desinstalación** en la configuración de la directiva del Agente de red.

La utilidad klmover requiere derechos de administrador local. La protección con contraseña para ejecutar la utilidad klmover se puede omitir para dispositivos que funcionan sin derechos de administrador local.

Al activar la opción **Utilizar contraseña de desinstalación**, también se activa la protección con contraseña para la herramienta Cleaner (cleaner.exe).

## Usar Kaspersky Security Network

En todas las directivas de las aplicaciones administradas y en las propiedades del Servidor de administración, recomendamos habilitar el uso de Kaspersky Security Network (KSN) y aceptar la Declaración de KSN. Cuando actualiza el Servidor de administración, puede aceptar la Declaración de KSN actualizada. En algunos casos, cuando el uso de servicios de nube está prohibido por la ley u otras regulaciones, puede deshabilitar KSN.

### Análisis periódico de dispositivos administrados

Recomendamos, para todos los grupos de dispositivos, crear una tarea que ejecute periódicamente un análisis completo de los dispositivos.

### Detección de nuevos dispositivos

Recomendamos establecer correctamente la configuración de detección de dispositivos: configure la integración con Active Directory y especifique intervalos de direcciones IP para detectar nuevos dispositivos.

Por motivos de seguridad, puede utilizar el grupo de administración predeterminado que incluye todos los dispositivos nuevos y las directivas predeterminadas que afectan a este grupo.

### Seleccionar una carpeta compartida

Si despliega el Servidor de administración en el dispositivo que ejecuta Windows con la selección de una carpeta compartida existente (que se usa, por ejemplo, para ubicar paquetes de instalación y almacenar bases de datos actualizadas), recomendamos asegurarse de que se otorguen derechos de lectura al grupo Todos y derechos de escritura al grupo KLAdmins.

## Mantenimiento del Servidor de administración

### Copia de seguridad de los datos del Servidor de administración

Las copias de seguridad de datos le permiten restaurar los datos del Servidor de administración sin pérdida de datos.

De forma predeterminada, se crea una tarea de copia de seguridad de datos automáticamente después de la instalación del Servidor de administración y se ejecuta periódicamente, guardando las copias de seguridad en el directorio adecuado.
La configuración de la tarea de copia de seguridad de datos se puede cambiar de la siguiente manera:

- La frecuencia de la copia de seguridad aumenta
- Se especifica un directorio especial para guardar copias
- Se modifican las contraseñas de las copias de seguridad

Si almacena copias de seguridad en un directorio especial distinto al directorio predeterminado, le recomendamos que limite la lista de control de acceso (ACL) de este directorio. Las cuentas del Servidor de administración y las cuentas de la base de datos del Servidor de administración deben tener acceso de escritura a este directorio.

### Mantenimiento del Servidor de administración

El mantenimiento del Servidor de administración le permite reducir el volumen de la base de datos y mejorar el rendimiento y la fiabilidad del funcionamiento de la aplicación. Le recomendamos realizar un mantenimiento del Servidor de administración por lo menos una vez a la semana.

El mantenimiento del Servidor de administración se lleva a cabo a través de la tarea especializada. La aplicación realiza las acciones siguientes durante el mantenimiento del Servidor de administración:

- Verifica si hay errores en la base de datos
- Reorganiza los índices de la base de datos
- Actualiza las estadísticas de la base de datos
- Reduce la base de datos si es necesario

### Instalación de actualizaciones del sistema operativo y actualizaciones de software de terceros

Enfatizamos nuestra recomendación de instalar de forma periódica actualizaciones de software para el sistema operativo y el software de terceros en el dispositivo del Servidor de administración.

Los dispositivos cliente no requieren una conexión continua al Servidor de administración, por lo que es seguro reiniciar el dispositivo del Servidor de administración después de instalar las actualizaciones. Todos los eventos registrados en los dispositivos cliente durante el tiempo de inactividad del Servidor de administración se envían al mismo una vez que se restablece la conexión.

## Transferencia de eventos a sistemas de terceros

### Supervisión e informes

Para dar una respuesta oportuna a los problemas de seguridad, recomendamos configurar las funciones de supervisión y generación de informes.

### Exportación de eventos a sistemas SIEM

Para obtener una detección rápida de problemas de seguridad antes de que se produzcan daños significativos, recomendamos usar la exportación de eventos en un sistema SIEM.

### Notificaciones por correo electrónico de eventos de auditoría

Kaspersky Security Center le permite recibir información sobre los eventos de funcionamiento del Servidor de administración y aplicaciones de Kaspersky instaladas en dispositivos administrados. Para obtener una respuesta oportuna ante emergencias, recomendamos configurar el Servidor de administración para enviar notificaciones sobre los eventos de auditoría, eventos críticos, eventos de fallos y advertencias que publica.

Dado que estos eventos tienen lugar dentro del sistema, se puede esperar que no sean muchos, algo que resulta muy cómodos para enviarlos por correo.

### Estadísticas de la función del Servidor de administración

Para responder oportunamente a cuestiones de seguridad, recomendamos configurar el envío de estadísticas de la función del Servidor de Administración a aplicaciones de terceros mediante el uso del Protocolo simple de administración de redes (SNMP).

# Recomendaciones de seguridad para sistemas de información de terceros

## Recomendaciones de seguridad de CIS Benchmarks

Al usar versiones de sistemas operativos, plataformas de virtualización o servidores de bases de datos compatibles con el Servidor de administración y el Agente de red, sugerimos que, de existir, aplique las prácticas de seguridad de la información recomendadas por el Center for Internet Security (CIS) para ajustar la configuración de estos sistemas de información

El Center for Internet Security (CIS) es una organización sin fines de lucro dedicada a mejorar la seguridad en el campo de la tecnología de la información. En particular, el CIS desarrolla y distribuye estándares de seguridad como CIS Controls y CIS Benchmarks. Estos estándares incluyen un conjunto de recomendaciones y prácticas para garantizar la seguridad de los sistemas de información.

El portal del CIS contiene recomendaciones para las versiones de los siguientes sistemas de información compatibles con el Servidor de administración y el Agente de red:

- Sistemas operativos de las siguientes familias:
  - Windows para equipos de escritorio
  - Windows para servidores
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS
- Plataformas de virtualización VMware
- Servidores de bases de datos:
  - Microsoft SQL Server
  - MySQL
  - MariaDB
  - PostgreSQL

### Recomendaciones de seguridad para el sistema operativo Astra Linux

Si utiliza el sistema operativo Astra Linux, siga las recomendaciones de seguridad descritas en el "libro rojo" correspondiente a su versión de Astra Linux.

### Recomendaciones de seguridad para el sistema operativo RED OS

Si utiliza el sistema operativo RED OS, siga las recomendaciones de seguridad de la guía del administrador descritas en la documentación oficial de RED OS.

## Recomendaciones para usar las aplicaciones de seguridad de Kaspersky

### Usar la contraseña de KLAdmin en Kaspersky Endpoint Security para Windows

Distintos usuarios con diferentes niveles de conocimientos informáticos pueden compartir un dispositivo con Kaspersky Endpoint Security para Windows instalado. Si los usuarios tienen acceso sin restricciones a Kaspersky Endpoint Security para Windows y sus configuraciones, el nivel general de protección del dispositivo puede verse reducido. La protección con contraseña le permite restringir el acceso de los usuarios a Kaspersky Endpoint Security para Windows, de acuerdo con los permisos otorgados (por ejemplo, permiso para salir de la aplicación).

Una de las formas de restringir el acceso a Kaspersky Endpoint Security para Windows y sus parámetros es usar una cuenta KLAdmin. La cuenta KLAdmin es una cuenta de administrador con acceso sin restricciones a Kaspersky Endpoint Security para Windows. La cuenta KLAdmin tiene derecho a realizar cualquier acción protegida con contraseña en Kaspersky Endpoint Security para Windows. Los permisos para la cuenta KLAdmin no se pueden revocar. Puede configurar la contraseña de la cuenta KLAdmin en las propiedades de la directiva de Kaspersky Endpoint Security para Windows. El administrador de Kaspersky Endpoint Security para Windows es totalmente responsable del uso seguro de esta contraseña. Si su organización tiene su propia directiva de contraseñas, siga las instrucciones de dicha directiva.

Estas son nuestras recomendaciones para proteger a la organización contra el robo de la contraseña de KLAdmin:

- **Requisitos generales**

  No utilice el nombre de la cuenta o parte del nombre como contraseña.

- **Requisitos mínimos sobre la longitud de la contraseña**

  Cree una contraseña de 10 caracteres o más.

- **Requisitos sobre el uso de varios tipos de caracteres**

  Establezca una contraseña compleja que contenga caracteres de diferentes categorías: letras minúsculas y mayúsculas, números y caracteres especiales.

- **Requisitos sobre la caducidad de la contraseña**

  Establezca la fecha mínima de caducidad de la contraseña en 90 días. Una nueva contraseña no debe coincidir con ninguna de las 24 contraseñas anteriores.

# Preparativos para el despliegue

Esta sección describe los pasos que debe completar antes de realizar el despliegue de Kaspersky Security Center.

## Planificación de la distribución de Kaspersky Security Center

Esta sección proporciona la información sobre las opciones más convenientes para el despliegue de los componentes de Kaspersky Security Center en la red de una organización, según los siguientes criterios:

- Número total de dispositivos.
- Unidades (oficinas locales, sucursales) que se separan a nivel organizacional o geográfico.
- Redes independientes conectadas por canales estrechos.
- Necesidad de acceso por Internet al Servidor de administración.

### Esquemas típicos para desplegar un sistema de protección

Esta sección describe los esquemas estándares de distribución de un sistema de protección con Kaspersky Security Center.

El sistema se debe proteger contra cualquier tipo del acceso no autorizado. Le recomendamos que instale todas las actualizaciones de seguridad disponibles para su sistema operativo antes de instalar la aplicación en su dispositivo y que proteja físicamente los Servidores de administración y los puntos de distribución.

Puede usar Kaspersky Security Center para distribuir un sistema de protección en una red corporativa por medio de los siguientes esquemas de distribución:

- Desplegar un sistema de protección a través de Kaspersky Security Center mediante uno de los siguientes métodos:
  - A través de la Consola de administración
  - A través de Kaspersky Security Center Web Console

  Las aplicaciones de Kaspersky se instalan de manera automática en los dispositivos cliente, que a su vez se conectan automáticamente al Servidor de administración mediante Kaspersky Security Center.

  El esquema de despliegue básico consiste en desplegar el sistema de protección a través de la Consola de administración. Kaspersky Security Center Web Console le permite iniciar la instalación de las aplicaciones de Kaspersky desde un navegador.

- Distribución de un sistema de protección de manera manual mediante los paquetes de instalación independientes creados en Kaspersky Security Center.

  La instalación de las aplicaciones de Kaspersky en los dispositivos cliente y en la estación de trabajo del administrador se realiza manualmente; la configuración para conectar los dispositivos cliente al Servidor de administración se define durante la instalación del Agente de red.

  Este método de despliegue se recomienda cuando no existe la posibilidad de realizar instalaciones remotas.

Kaspersky Security Center también le permite desplegar su sistema de protección mediante las directivas de grupo de Microsoft Active Directory.

## Información acerca de la planificación del despliegue de Kaspersky Security Center en la red de una organización

Un Servidor de administración puede admitir un máximo de 100 000 dispositivos. Cuando el número total de dispositivos en la red de una organización supera los 100 000, resulta necesario instalar varios Servidores de administración en esa red y combinarlos en una jerarquía para lograr una administración centralizada conveniente.

Si una organización incluye oficinas locales remotas a gran escala (sucursales) con sus propios administradores, es útil instalar Servidores de administración en dichas oficinas. De otra forma, esas oficinas se deben ver como redes separadas conectadas por canales de bajo rendimiento, consulte la sección "Configuración estándar: pocas oficinas a gran escala ejecutadas por sus propios administradores".

Al usar redes separadas conectadas a canales estrechos, puede ahorrarse tráfico al asignar uno o varios Agentes de red para que funcionen como puntos de distribución (consulte tabla para la evaluación del número de puntos de distribución). En este caso, todos los dispositivos en una red separada recuperan actualizaciones desde tales centros de actualización locales. Los puntos de distribución reales pueden descargar actualizaciones tanto desde el Servidor de administración (escenario predeterminado) como desde servidores de Kaspersky en Internet (ver la sección "Configuración estándar: varias oficinas pequeñas remotas").

La sección "Configuraciones estándares de Kaspersky Security Center" proporciona descripciones detalladas de las configuraciones estándares de Kaspersky Security Center. Al planificar el despliegue, elija la configuración estándar más conveniente, según la estructura de la organización.

En la etapa de planificación del despliegue, es necesario tener en cuenta la asignación del certificado especial X.509 al Servidor de administración. La asignación del certificado X.509 al Servidor de administración puede ser útil en los casos siguientes (lista parcial):

- Inspección del tráfico de la capa de sockets seguros (SSL) por medio de un proxy de cancelación de la SSL, o para usar un proxy inverso
- Integración con la infraestructura de claves públicas (PKI) de una organización
- Para especificar los valores requeridos de los campos del certificado
- Para proporcionar la solidez de cifrado deseada del certificado

## Selección de una estructura para la protección de una empresa

La selección de una estructura para la protección de una organización depende de los siguientes factores:

- Topología de red de la organización.
- Estructura organizativa.
- Número de empleados a cargo de la protección de la red y asignación de sus responsabilidades.
- Recursos de hardware que se pueden asignar a los componentes de administración de protección.
- Volumen de trabajo de los canales de comunicación que se puede asignar para el mantenimiento de los componentes de protección en la red de la organización.
- Límites de tiempo para ejecutar las operaciones administrativas críticas en la red de la organización. Las operaciones administrativas críticas incluyen, por ejemplo, la distribución de bases de datos antivirus y la modificación de las directivas de los dispositivos cliente.

Al seleccionar una estructura de protección, se recomienda que, en primer lugar, se estimen los recursos de red y hardware disponibles que se pueden usar para la operación de un sistema de protección centralizado.

Para analizar la red e infraestructura del hardware, se recomienda que siga el proceso a continuación:

1. Defina la siguiente configuración de la red en la que se desplegará la protección:
   - Número de segmentos de red.
   - Velocidad de los canales de comunicación entre segmentos de red individuales.
   - Número de dispositivos administrados en cada segmento de red.
   - Volumen de trabajo de cada canal de comunicación que se puede asignar para mantener operativa la protección.
2. Determina el tiempo máximo permitido para la ejecución de operaciones administrativas clave para todos los dispositivos administrados.
3. Analice la información d los pasos 1 y 2, así como los datos de las pruebas de carga del sistema de administración. Según el análisis, responda las siguientes preguntas:
   - ¿Es posible prestar servicio a todos los clientes con un solo Servidor de administración o se requiere una jerarquía de Servidores de administración?
   - ¿Qué configuración de hardware de los Servidores de administración se requiere para manejar todos los clientes dentro de los plazos especificados en el paso 2?
   - ¿Es preciso usar los puntos de distribución para reducir la carga en los canales de comunicación?

Si obtiene las respuestas a las preguntas del paso 3 anterior, podrá compilar un conjunto de estructuras permitidas de protección de la organización.

En la red de la organización, puede usar una de las siguientes estructuras de protección estándares:

- Un Servidor de administración. Todos los dispositivos cliente están conectados a un solo Servidor de administración. El Servidor de administración funciona como el punto de distribución.
- Un Servidor de administración con puntos de distribución. Todos los dispositivos cliente están conectados a un solo Servidor de administración. Algunos de los dispositivos cliente conectados a una red funcionan como puntos de distribución.
- Jerarquía de Servidores de administración. Se asigna un Servidor de administración a cada uno de los segmentos de la red y estos pasan a formar una jerarquía general de Servidores de administración. El Servidor de administración principal funciona como punto de distribución.
- Jerarquía de Servidores de administración con puntos de distribución. Se asigna un Servidor de administración a cada uno de los segmentos de la red y estos pasan a formar una jerarquía general de Servidores de administración. Algunos de los dispositivos cliente conectados a una red funcionan como puntos de distribución.

## Configuraciones estándares de Kaspersky Security Center

Esta sección describe las configuraciones estándares siguientes usadas para la distribución de componentes de Kaspersky Security Center en la red de la organización:

- Oficina única
- Unas pocas oficinas a gran escala, que están geográficamente separadas y son dirigidas por sus propios administradores
- Varias oficinas pequeñas, que están geográficamente separadas

## Configuración estándar: oficina única

Puede haber uno o varios Servidores de administración instalados en la red de la organización. El número de Servidores de administración se puede seleccionar según el hardware disponible o el número total de dispositivos administrados.

Un Servidor de administración puede admitir un máximo de 100 000 dispositivos. Debe considerar la posibilidad de aumentar el número de dispositivos administrados en el futuro próximo: puede ser útil conectar un número levemente menor de dispositivos a un solo Servidor de administración.

Los Servidores de administración pueden instalarse en la red interna o en la DMZ; la decisión dependerá de si se necesita o no acceder a los Servidores de administración por Internet.

Si se utilizan varios servidores, se recomienda que los combine en una jerarquía. La utilización de una jerarquía de Servidores de administración le permite evitar directivas y tareas duplicadas y gestionar el conjunto entero de dispositivos administrados como si estuvieran administrados por un Servidor de administración único (es decir, buscar dispositivos, crear selecciones de dispositivos y crear informes).

## Configuración estándar: algunas oficinas a gran escala dirigidas por sus propios administradores

Si la organización tiene unas pocas oficinas grandes geográficamente separadas, debe considerar la opción de desplegar Servidores de administración en cada una de ellas. Se pueden desplegar uno o varios Servidores de administración por oficina, según la cantidad de dispositivos cliente y el hardware disponibles. En este caso, cada una de las oficinas se puede ver como una "Configuración estándar: oficina única". Para facilitar la administración, le recomendamos que combine todos los Servidores de administración en una jerarquía (de ser posible, de varios niveles).

Si hay empleados que se mueven entre distintas oficinas con sus dispositivos (computadoras portátiles), cree perfiles de conexión del Agente de red en la directiva del Agente de red. Los perfiles de conexión del Agente de red solo son compatibles con dispositivos Windows y macOS.

## Configuración estándar: varias oficinas remotas pequeñas

Esta configuración estándar es útil para una oficina central y muchas oficinas remotas pequeñas que pueden comunicarse con la oficina central por Internet. Cada una de las oficinas remotas puede localizarse detrás de la Traducción de la Dirección de red (NAT), es decir, no puede establecerse ninguna conexión entre dos oficinas remotas, dado que están aisladas.

Debe desplegarse un Servidor de administración en la oficina central y deben asignarse uno o varios puntos de distribución al resto de las oficinas. Si las oficinas están conectadas a través de Internet, puede ser útil crear una tarea *Descargar actualizaciones a los repositorios de puntos de distribución* para los puntos de distribución, de modo que descarguen las actualizaciones directamente desde los servidores de Kaspersky, carpeta local o de la red, no desde el Servidor de administración.

Si algunos dispositivos en una oficina remota no tienen acceso directo al Servidor de administración (por ejemplo, el acceso al Servidor de administración se proporciona mediante Internet, pero algunos dispositivos no tienen acceso a Internet), los puntos de distribución se deben cambiar al modo de puerta de enlace de conexión. En este caso, los Agentes de red de los dispositivos en la oficina remota se conectarán, para realizar una sincronización adicional, con el Servidor de administración, pero a través de la puerta de enlace, no directamente.

Como es muy probable que el Servidor de administración no pueda realizar un sondeo de la red de la oficina remota, puede ser útil transferir esta función a un punto de distribución.

El Servidor de administración no podrá enviar notificaciones al puerto UDP 15000 a dispositivos administrados ubicados detrás de la NAT en la oficina remota. Para resolver este problema, puede habilitar el modo de conexión continua al Servidor de administración en las propiedades de los dispositivos que actúan como puntos de distribución (casilla **No desconectar del Servidor de administración**). Este modo está disponible si el número total de puntos de distribución no supera los 300. Utilice servidores push para asegurarse de que haya una conectividad continua entre un dispositivo administrado y el Servidor de administración. Consulte el siguiente tema para obtener más información: Uso de un punto de distribución como servidor push.

## Seleccionar un DBMS para el Servidor de administración

Al seleccionar el sistema de administración de bases de datos (DBMS) para utilizarlo en un Servidor de administración, debe tener en cuenta el número de dispositivos cubiertos por el Servidor de administración.

La siguiente tabla enumera las opciones de DBMS válidas, así como las recomendaciones y las restricciones en su uso.

Recomendaciones y restricciones en DBMS

| DBMS | Recomendaciones y restricciones |
|---|---|
| SQL Server Express Edition 2016 o posterior | Utilice este DBMS si planea ejecutar un solo Servidor de administración para menos de 10 000 dispositivos.<br>Se recomienda deshabilitar la Tarea del inventario del software y deshabilitar (en la configuración de directivas de Kaspersky Endpoint Security) las notificaciones del Servidor de administración en las aplicaciones iniciadas.<br>Puede limitar el número máximo de eventos en el repositorio de eventos para evitar el desbordamiento de la base de datos.<br>Consulte el siguiente tema para más detalles: Evaluación de espacio de la base de datos.<br>El uso simultáneo del DBMS de SQL Server Express Edition por el Servidor de administración y otras aplicaciones está estrictamente prohibido.<br>La base de datos de Microsoft SQL Express no es compatible con la tarea **Sincronización con Windows Update**. |
| Edición de SQL Server local, no Express, 2016 o posterior | Sin limitaciones. |
| Edición de SQL Server remota, no Express, 2016 o posterior | Solo es válido si ambos dispositivos están en el mismo dominio de Windows®; Si los dominios difieren, se debe establecer una relación de confianza bidireccional entre ellos. |
| MySQL 5.5, 5.6 o 5.7 local o remoto (ya no se admiten las versiones 5.5.1, 5.5.2, 5.5.3, 5.5.4 y 5.5.5 de MySQL) | Utilice este DBMS si planea ejecutar un solo Servidor de administración para menos de 10 000 dispositivos.<br>Se recomienda deshabilitar la Tarea del inventario del software y deshabilitar (en la configuración de directivas de Kaspersky Endpoint Security) las notificaciones del Servidor de administración en las aplicaciones iniciadas. Consulte el siguiente tema para más detalles: Evaluación de espacio de la base de datos. |
| MySQL 8.0.20 o versión posterior local o remoto | Utilice este DBMS si planea ejecutar un solo Servidor de administración para menos de 50 000 dispositivos.<br>Se recomienda deshabilitar la Tarea del inventario del software y deshabilitar (en la configuración de directivas de Kaspersky Endpoint Security) las notificaciones del Servidor de administración en las aplicaciones iniciadas. Consulte el siguiente tema para más detalles: Evaluación de espacio de la base de datos. |

| DBMS | Recomendaciones y restricciones |
| --- | --- |
| MariaDB local o remota (ver versiones compatibles) | Utilice este DBMS si planea ejecutar un solo Servidor de administración para menos de 20 000 dispositivos.<br>Se recomienda deshabilitar la Tarea del inventario del software y deshabilitar (en la configuración de directivas de Kaspersky Endpoint Security) las notificaciones del Servidor de administración en las aplicaciones iniciadas. Consulte el siguiente tema para más detalles: Evaluación de espacio de la base de datos. |
| PostgreSQL, Postgres Pro (ver versiones compatibles) | Utilice uno de estos DBMS si planea ejecutar un solo Servidor de administración para menos de 50 000 dispositivos.<br>Se recomienda deshabilitar la Tarea del inventario del software y deshabilitar (en la configuración de directivas de Kaspersky Endpoint Security) las notificaciones del Servidor de administración en las aplicaciones iniciadas. Consulte el siguiente tema para más detalles: Evaluación de espacio de la base de datos. |

Si está utilizando SQL Server 2019 como DBMS y no tiene el parche acumulativo CU12 o posterior, debe realizar lo siguiente después de instalar Kaspersky Security Center:

1. Conéctese a SQL Server con SQL Management Studio.
2. Ejecute los siguientes comandos (si elige un nombre diferente para la base de datos, use ese nombre en lugar de KAV):

```
USE KAV
GO
ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
GO
```

3. Reinicie el servicio SQL Server 2019.

De lo contrario, el uso de SQL Server 2019 puede generar errores, como "There is insufficient system memory in resource pool 'internal' to run this query" (Memoria de sistema insuficiente en el grupo de recursos interno para ejecutar esta consulta).

## Configurar el servidor MariaDB x64 para trabajar con Kaspersky Security Center 15.1

Para configurar correctamente el servidor PostgreSQL o Postgres Pro para que funcione con Kaspersky Security Center, debe usar los parámetros del servidor predeterminados, con la excepción de los parámetros del servidor que se especifican en este artículo.

Kaspersky Security Center 15.1 es compatible con el DBMS MariaDB. Para obtener más información sobre las versiones compatibles de MariaDB, consulte la sección Requisitos de hardware y software.

Si utiliza el DBMS de MariaDB para Kaspersky Security Center, active la compatibilidad del almacenamiento InnoDB y MEMORY y las codificaciones UTF-8 y UCS-2.

## Configuraciones recomendadas del archivo my.ini

*Para configurar el archivo my.ini:*

1. Abra el archivo my.ini en un editor de texto.

2. Agregue las siguientes líneas en la sección `[mysqld]` del archivo my.ini:

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=< el valor real no debe ser inferior al 80 % del tamaño
esperado de la base de datos KAV >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
sql_mode="STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"
```

   El valor de `innodb_buffer_pool_size` no debe ser inferior al 80 por ciento del tamaño esperado de la base de datos KAV. Tenga en cuenta que la memoria especificada se asigna en el momento en que se inicia el servidor. Si el tamaño de la base de datos es inferior al tamaño especificado para el búfer, se asignará únicamente la memoria necesaria. Si utiliza MariaDB 10.4.3 o una versión anterior, la cantidad de memoria asignada será, en la práctica, aproximadamente un 10 % superior al tamaño especificado para el búfer.

   Se recomienda utilizar el valor del parámetro `innodb_flush_log_at_trx_commit=0`, porque los valores "1" o "2" afectan negativamente la velocidad de funcionamiento de MariaDB. Asegúrese de que el parámetro `innodb_file_per_table` esté establecido en `1`.

   Para MariaDB 10.1, ingrese adicionalmente las siguientes líneas en la sección [mysqld]:

```
innodb_file_format='Barracuda'
innodb_default_row_format=dynamic
innodb_large_prefix=1
```

   Para MariaDB 10.6, ingrese adicionalmente las siguientes líneas en la sección [mysqld]:

```
optimizer_prune_level=0
optimizer_search_depth=8
```

De manera predeterminada, los complementos optimizadores `join_cache_incremental`, `join_cache_hashed` y `join_cache_bka` están habilitados. Si estos complementos no están habilitados, debe habilitarlos.

*Para comprobar si los complementos optimizadores están habilitados o no:*

1. En la consola cliente MariaDB, ejecute el comando:

   ```
   SELECT @@optimizer_switch;
   ```

2. Compruebe que la salida contenga las siguientes líneas:

   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```

   Si estas líneas están presentes y tienen el valor `on`, quiere decir que están habilitados los complementos optimizadores.

   Si estas líneas faltan o tienen el valor `off`, haga lo siguiente:

   1. Abra el archivo my.ini en un editor de texto.

   2. Agregue las siguientes líneas en la sección `[mysqld]` del archivo my.ini:

      ```
      optimizer_switch='join_cache_incremental=on'
      optimizer_switch='join_cache_hashed=on'
      optimizer_switch='join_cache_bka=on'
      ```

Los complementos `join_cache_incremental`, `join_cache_hash` y `join_cache_bka` están habilitados.

## Configurar el servidor MySQL x64 para que funcione con Kaspersky Security Center 15.1

Para configurar correctamente el servidor PostgreSQL o Postgres Pro para que funcione con Kaspersky Security Center, debe usar los parámetros del servidor predeterminados, con la excepción de los parámetros del servidor que se especifican en este artículo.

Si utiliza el DBMS de MySQL para Kaspersky Security Center, active la compatibilidad del almacenamiento InnoDB y MEMORY y las codificaciones UTF-8 y UCS-2.

## Configuraciones recomendadas del archivo my.ini

*Para configurar el archivo my.ini:*

1. Abra el archivo my.ini en un editor de texto.

2. Agregue las siguientes líneas en la sección `[mysqld]` del archivo my.ini:

```
sort_buffer_size=10M
join_buffer_size=20M
tmp_table_size=600M
max_heap_table_size=600M
key_buffer_size=200M
innodb_buffer_pool_size=<el valor real no debe ser inferior al 80 % del tamaño esperado de la base de datos KAV>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (en la mayoría de los casos, el servidor utiliza transacciones pequeñas)
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

   Tenga en cuenta que la memoria especificada en el valor `innodb_buffer_pool_size` se asigna al inicio del servidor. Si el tamaño de la base de datos es más pequeño que el tamaño del búfer especificado, solo se asigna la memoria necesaria. El tamaño real de la memoria asignada es aproximadamente un 10 por ciento mayor que el tamaño del búfer especificado. Consulte la documentación de MySQL para obtener más detalles.

   Se recomienda utilizar el valor del parámetro `innodb_flush_log_at_trx_commit = 0`, porque los valores "1" o "2" afectan negativamente la velocidad de funcionamiento de MySQL. Asegúrese de que el parámetro `innodb_file_per_table` esté establecido en `1`.

## Configurar el servidor PostgreSQL o Postgres Pro para trabajar con Kaspersky Security Center 15.1

Para configurar correctamente el servidor PostgreSQL o Postgres Pro para que funcione con Kaspersky Security Center, debe usar los parámetros del servidor predeterminados, con la excepción de los parámetros del servidor que se especifican en este artículo.

Kaspersky Security Center 15.1 es compatible con los DBMS PostgreSQL y Postgres Pro. Si usa uno alguno de estos DBMS, recomendamos que configure los parámetros del mismo para que funcione en forma óptima con Kaspersky Security Center Linux.

La ruta predeterminada al archivo de configuración es: `C:\Program Files\PostgreSQL\<VERSIÓN>\data\postgresql.conf`

Parámetros recomendados para PostgreSQL y Postgres Pro:

- `shared_buffers` = 25 por ciento del valor de RAM del dispositivo en el que está instalado el DBMS

  Si el dispositivo tiene menos de 1 GB de memoria RAM, deje el valor predeterminado.

- `max_stack_depth = 2MB`

- `temp_buffers = 24MB`
- `work_mem = 16MB`
- `max_connections = 151`
- `max_parallel_workers_per_gather = 0`
- `maintenance_work_mem = 128MB`

Asegúrese de que el parámetro `standard_conforming_strings` esté establecido en el valor predeterminado `on`. Vuelva a cargar la configuración o reinicie el servidor después de actualizar el archivo postgresql.conf. Consulte la documentación de PostgreSQL para obtener más detalles.

Si utiliza Postgres Pro 15.7 o Postgres Pro 15.7.1, desactive el parámetro `enable_compound_index_stats`:

```
enable_compound_index_stats = off
```

Para obtener información sobre los parámetros del servidor PostgreSQL y Postgres Pro y sobre cómo especificarlos, consulte la documentación DBMS correspondiente.

Consulte el siguiente tema para obtener detalles sobre cómo crear y configurar cuentas para PostgreSQL y Postgres Pro: Configuración de cuentas para trabajar con PostgreSQL y Postgres Pro.

## Administración de dispositivos móviles con Kaspersky Endpoint Security para Android

Los dispositivos móviles con Kaspersky Endpoint Security para Android™ instalado (denominados, en lo sucesivo, dispositivos KES) se administran por medio del Servidor de administración. Kaspersky Security Center admite las siguientes funciones para administrar dispositivos KES:

- Manejo de dispositivos móviles como dispositivos cliente:
  - Membrecía en grupos de administración
  - Supervisión, por ejemplo, ver estados, eventos e informes
  - Modificación de la configuración local y asignación de directivas para Kaspersky Endpoint Security para Android
- Envío de comandos en modo centralizado
- Instalación de paquetes de aplicaciones móviles remotamente

El Servidor de administración administra los dispositivos KES mediante TLS, puerto TCP 13292.

## Suministro de acceso a Internet al Servidor de administración

Los casos siguientes requieren acceso a Internet para el Servidor de administración:

- Actualizar periódicamente las bases de datos, los módulos de software y las aplicaciones de Kaspersky
- Actualización de software de terceros

  De forma predeterminada, el Servidor de administración no requiere conexión a Internet para instalar las actualizaciones de software de Microsoft en los dispositivos administrados. Los dispositivos administrados pueden descargar las actualizaciones de software de Microsoft directamente de los servidores de Microsoft Update, por ejemplo, o de un servidor Windows Server que esté desplegado en la red de la organización y que tenga Windows Server Update Services (WSUS) habilitado. El Servidor de administración debe tener conexión a Internet en los siguientes casos:

  - Al usar un Servidor de administración como servidor WSUS
  - Para instalar actualizaciones de software de terceros que no sean software de Microsoft
- Reparación de vulnerabilidades en el software de terceros

  Se requiere conexión a Internet para que el Servidor de administración realice las siguientes tareas:

  - Hacer una lista de reparaciones recomendadas para vulnerabilidades en el software de Microsoft. Los especialistas de Kaspersky crean y actualizan periódicamente esta lista.
  - Reparar vulnerabilidades en software de terceros que no sean Microsoft.
- Administración de dispositivos (portátiles) de usuarios fuera de la oficina
- Administración de dispositivos en oficinas remotas
- Interacción con Servidores de administración principales o secundarios localizados en oficinas remotas
- Administración de dispositivos móviles

Esta sección describe modos habituales de proporcionar acceso al Servidor de administración a través de Internet. Cada uno de los casos que se centra en proporcionar acceso a Internet al Servidor de administración puede requerir un certificado dedicado para el Servidor de administración.

### Acceso a Internet: Servidor de administración en una red local

Si el Servidor de administración está ubicado dentro de la intranet de una organización, puede hacer que el puerto TCP 13000 del Servidor de administración sea accesible desde fuera mediante el redireccionamiento de puertos. Si se requiere la administración de dispositivos móviles, puede hacer accesible el puerto 13292 TCP.

### Acceso a Internet: Servidor de administración en la zona desmilitarizada (DMZ)

Si el Servidor de administración está ubicado en la DMZ de la red de la organización, no tiene acceso a la intranet de la organización. Por lo tanto, las limitaciones siguientes se aplican:

- El Servidor de administración no puede detectar dispositivos nuevos.
- El Servidor de administración no puede realizar el despliegue inicial del Agente de red a través de la instalación forzada en dispositivos en la red interna de la organización.

Esto solo se aplica a la instalación inicial del Agente de red. Algunas otras actualizaciones del Agente de red o la instalación de la aplicación de seguridad pueden ser, sin embargo, realizadas por el Servidor de administración. Al mismo tiempo, el despliegue inicial del Agente de red puede realizarse por otros medios; por ejemplo, a través de directivas de grupo de Microsoft® Active Directory®.

- El Servidor de administración no puede enviar notificaciones a dispositivos administrados mediante el puerto UDP 15000, lo que no es crítico para el funcionamiento de Kaspersky Security Center.

- El Servidor de administración no puede realizar un sondeo de Active Directory. Sin embargo, los resultados del sondeo de Active Directory no son necesarios en la mayor parte de los casos.

Si las limitaciones indicadas anteriormente se ven como críticas, pueden eliminarse usando puntos de distribución ubicados dentro de la red de la organización:

- Para realizar el despliegue inicial en dispositivos sin el Agente de red, primero instale el Agente de red en uno de los dispositivos y luego asígnele el estado de punto de distribución. Como resultado, la instalación inicial del Agente de red en otros dispositivos será realizada por el Servidor de administración a través de este punto de distribución.

- Para detectar dispositivos nuevos en la red interna de la organización y realizar un sondeo de Active Directory, debe habilitar los métodos correspondientes de descubrimiento de dispositivos en uno de los puntos de distribución.

Para garantizar el envío correcto de notificaciones al puerto UDP 15000 en dispositivos administrados ubicados dentro de la intranet de la organización, debe abarcar la red completa de puntos de distribución. En las propiedades de los puntos de distribución que se asignaron, seleccione la casilla de verificación **No desconectar del Servidor de administración**. Como resultado, el Servidor de administración establecerá una conexión continua con los puntos de distribución y estos podrán enviar notificaciones al puerto UDP 15 000 en dispositivos dentro de la red interna de la organización (puede ser una red IPv4 o IPv6).

## Acceso a Internet: Agente de red en modo de puerta de enlace de conexión en DMZ

El Servidor de administración se puede localizar en la red interna de la organización, y en la DMZ de esa red puede haber un dispositivo con Agente de red que se ejecute como puerta de enlace de conexión con conectividad inversa (el Servidor de administración establece una conexión con el Agente de red). En este caso, las condiciones siguientes se deben cumplir para asegurar el Acceso a Internet:

- El Agente de red debe estar instalado en el dispositivo ubicado en la DMZ. Cuando instale el Agente de red, en la ventana **Puerta de enlace de conexión** del Asistente de instalación, seleccione **Usar el Agente de red como una puerta de enlace de conexión en la DMZ**.

- El dispositivo designado como puerta de enlace de conexión debe agregarse como punto de distribución. Cuando agregue la puerta de enlace de conexión, en la ventana **Agregar un punto de distribución**, elija la opción **Seleccionar → Agregar puerta de enlace de conexión en la DMZ por dirección**.

- A fin de utilizar una conexión a Internet para conectar dispositivos de escritorio externos al Servidor de administración, se debe corregir el paquete de instalación del Agente de red. En las propiedades del paquete de instalación creado, seleccione **Avanzado → Conectarse al Servidor de administración mediante una puerta de enlace de conexión** y especifique la dirección de la puerta de enlace que acaba de crear.

Para la puerta de enlace de conexión en la DMZ, el Servidor de administración crea un certificado firmado con el certificado del Servidor de administración. Si el administrador decide asignar un certificado personalizado al Servidor de administración, debe hacerlo antes de crear una puerta de enlace de conexión en la DMZ.

Si algunos empleados usan computadoras portátiles que pueden conectarse al Servidor de administración desde la red local o mediante Internet, puede ser útil crear una regla de cambio para el Agente de red en la directiva del Agente de red.

## Acerca de los puntos de distribución

Los dispositivos que tengan instalado el Agente de red pueden utilizarse como punto de distribución. En este modo, el Agente de red puede realizar las funciones siguientes:

- Distribuir actualizaciones (estas se pueden obtener desde el Servidor de administración o desde los servidores de actualización de Kaspersky). En este último caso, debe crearse la tarea *Descargar actualizaciones en los repositorios de puntos de distribución* para el dispositivo que sirve como punto de distribución:
  - Instalar software (incluido el Agente de red, durante el despliegue inicial) en otros dispositivos.
  - Sondear la red para detectar nuevos dispositivos y actualizar la información disponible sobre los dispositivos de los que ya se tenía conocimiento. Un punto de distribución puede aplicar los mismos métodos de descubrimiento de dispositivos que el Servidor de administración.

El despliegue de puntos de distribución en la red de una organización cumple los siguientes objetivos:

- Reduce la carga en el Servidor de administración.
- Optimiza el tráfico.
- Proporciona al Servidor de administración acceso a dispositivos en puntos poco accesibles de la red de la organización. La disponibilidad de un puntos de distribución en la red detrás de la NAT (con relación al Servidor de administración) permite que el Servidor de administración realice las siguientes acciones:
  - Envíe notificaciones a dispositivos mediante UDP en la red IPv4 o IPv6.
  - Sondee la red IPv4 o IPv6.
  - Realizar el despliegue inicial.
  - Actúe como un servidor push.

Un punto de distribución se asigna a un grupo de administración. En este caso, la cobertura del punto de distribución incluye todos los dispositivos dentro del grupo de administración y todos sus subgrupos. Sin embargo, el dispositivo que funciona como el punto de distribución no puede incluirse en el grupo de administración al cual se ha asignado.

Puede hacer que un punto de distribución funcione como una puerta de enlace de conexión. En este caso, los dispositivos en la cobertura del punto de distribución se conectarán al Servidor de administración a través de la puerta de enlace, no directamente. Este modo puede ser útil en situaciones que no permitan establecer una conexión directa entre el Servidor de administración y los dispositivos administrados.

Si utiliza un dispositivo basado en Linux como punto de distribución, recomendamos encarecidamente aumentar el límite de descriptores de archivos para el servicio klnagent, ya que si el alcance del punto de distribución incluye muchos dispositivos, la cantidad máxima predeterminada de archivos que se pueden abrir puede no ser suficiente.

## Aumento del límite de descriptores de archivos para el servicio klnagent

Si el alcance de un punto de distribución con Linux incluye muchos dispositivos, el límite predeterminado de archivos que se pueden abrir (descriptores de archivos) puede resultar insuficiente. Para evitar problemas, puede aumentar el límite de descriptores de archivos para el servicio klnagent.

*Para aumentar el límite de descriptores de archivos para el servicio klnagent:*

1. En el dispositivo basado en Linux que actúa como punto de distribución, abra el `/lib/systemd/system/klnagent64.service` archivo y, a continuación, especifique los límites rígidos y flexibles de los descriptores de archivo en el `LimitNOFILE` parámetro del `[Service]` sección:

   `LimitNOFILE=<límite de recursos blando>:<límite de recursos duro>`

   Por ejemplo, `LimitNOFILE=32768:131072`. Tenga en cuenta que el límite blando de los descriptores de archivos debe ser inferior o igual al límite duro.

2. Ejecute el siguiente comando para asegurarse de que los parámetros se hayan indicado correctamente:

   `systemd-analyze verify klnagent64.service`

   Si los parámetros no se indicaron correctamente, el comando puede generar uno de los siguientes errores:

   - `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

     Si ve este error, los símbolos de la línea `LimitNOFILE` no están indicados correctamente Revise y corrija la línea que ingresó.

   - `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

     Si ve este error, el límite blando ingresado para los descriptores de archivos es superior al límite duro. Revise la línea ingresada y asegúrese de que el límite blando que defina para los descriptores de archivos sea inferior o igual al límite duro.

3. Ejecute el siguiente comando para volver a cargar el proceso systemd:

   `systemctl daemon-reload`

4. Ejecute el siguiente comando para reiniciar el servicio del Agente de red:

   `systemctl restart klnagent`

5. Ejecute el siguiente comando para asegurarse de que los parámetros indicados se apliquen correctamente:

   `less /proc/<Id de proceso nagent>/limits`

   donde el parámetro `<Id de proceso nagent>` es el identificador del proceso del Agente de Red. Puede ejecutar el siguiente comando para obtener el identificador:

   `ps -ax | grep klnagent`

Como resultado, se aumentará el límite de archivos que se pueden abrir en el punto de distribución con Linux.

## Cálculo de la cantidad de puntos de distribución y su configuración

Cuantos más dispositivos cliente contiene una red, más puntos de distribución se requieren. Le recomendamos que no deshabilite la asignación automática de puntos de distribución. Cuando se habilita la asignación automática de puntos de distribución, el Servidor de administración asigna puntos de distribución si el número de dispositivos cliente es bastante grande y define su configuración.

## La utilización de puntos de distribución exclusivamente asignados

Si planea usar ciertos dispositivos específicos como puntos de distribución (es decir, servidores asignados exclusivamente), puede optar por no usar la asignación automática de puntos de distribución. En este caso, compruebe que los dispositivos a los que planea hacer puntos de distribución tengan el volumen suficiente de espacio libre en disco, que no se apaguen con frecuencia y que tengan el modo de suspensión desactivado.

Número de puntos de distribución designados exclusivamente en una red que contiene un único segmento de red, en función del número de dispositivos en red

| Número de dispositivos cliente en el segmento de red | Número de puntos de distribución |
|---|---|
| Menos de 300 | 0 (no corresponde utilizar puntos de distribución) |
| Más de 300 | Aceptable: (N / 10 000 + 1), recomendado: (N / 5000 + 2), donde N es el número de dispositivos conectados a la red |

Número de puntos de distribución designados exclusivamente en una red que contiene múltiples segmentos de red, en función del número de dispositivos en red

| Número de dispositivos cliente por segmento de red | Número de puntos de distribución |
|---|---|
| Menos de 10 | 0 (no corresponde utilizar puntos de distribución) |
| 10–100 | 1 |
| Más de 100 | Aceptable: (N / 10 000 + 1), recomendado: (N / 5000 + 2), donde N es el número de dispositivos conectados a la red |

## Uso de dispositivos cliente estándar (estaciones de trabajo) como puntos de distribución

Si planea usar dispositivos cliente estándar (es decir, estaciones de trabajo) como puntos de distribución, le recomendamos que siga los lineamientos de las siguientes tablas. Al designar los puntos de distribución según estas recomendaciones, evitará las sobrecargas en los canales de comunicación y en el Servidor de administración.

Número de estaciones de trabajo designadas como puntos de distribución en una red que contiene un único segmento de red, en función del número de dispositivos en red

| Número de dispositivos cliente en el segmento de red | Número de puntos de distribución |
|---|---|
| Menos de 300 | 0 (no corresponde utilizar puntos de distribución) |
| Más de 300 | (N / 300 + 1), donde N es el número de dispositivos en red; debe haber al menos 3 puntos de distribución |

Número de estaciones de trabajo designadas como puntos de distribución en una red que contiene múltiples segmentos de red, en función del número de dispositivos en red

| Número de dispositivos cliente por segmento de red | Número de puntos de distribución |
|---|---|
| Menos de 10 | 0 (no corresponde utilizar puntos de distribución) |
| 10–30 | 1 |

| Número de dispositivos cliente por segmento de red | Número de puntos de distribución |
|---|---|
| 31–300 | 2 |
| Más de 300 | (N / 300 + 1), donde N es el número de dispositivos en red; debe haber al menos 3 puntos de distribución |

Cuando un punto de distribución se encuentra apagado o no está disponible por algún motivo, los dispositivos administrados en su alcance pueden obtener actualizaciones del Servidor de administración.

## Jerarquía de Servidores de administración

Un MSP puede ejecutar varios Servidores de administración. Puede ser poco conveniente administrar varios Servidores de administración independientes, por lo que se puede aplicar una jerarquía. La configuración "principal/secundario" de dos Servidores de administración proporciona las opciones siguientes:

- Un Servidor de administración secundario hereda directivas y tareas del Servidor de administración principal. De esta forma se previene la duplicación de parámetros.
- Las selecciones de dispositivos en el Servidor de administración principal pueden incluir dispositivos desde los Servidores de administración secundarios.
- Los informes sobre el Servidor de administración principal pueden contener datos (incluida información detallada) de los Servidores de administración secundarios.

El Servidor de administración principal solo recibe datos de Servidores de administración secundarios no virtuales dentro del alcance de las opciones antes enumeradas. Esta limitación no se aplica a los Servidores de administración virtuales, que comparten la base de datos con su Servidor de administración principal.

## Servidores de administración virtuales

Sobre la base de un Servidor de administración físico, se pueden crear varios Servidores de administración virtual, los que serán similares a los Servidores de administración secundarios. En comparación con el modelo de acceso discrecional, que se basa en listas de control de acceso (ACL), el modelo del Servidor de administración virtual es más funcional y proporciona un mayor nivel de aislamiento. Además de una estructura dedicada de grupos de administración para dispositivos asignados con directivas y tareas, cada Servidor de administración virtual presenta su propio grupo de dispositivos no asignados, sus propios conjuntos de informes, dispositivos seleccionados y eventos, paquetes de instalación, reglas de traslado, etc. El alcance funcional de los Servidores de administración virtuales puede ser utilizado tanto por proveedores de servicios (xSP) para maximizar el aislamiento de los clientes como por organizaciones a gran escala con flujos de trabajo sofisticados y numerosos administradores.

Los Servidores de administración virtual son muy similares a los Servidores de administración secundarios, pero con las distinciones siguientes:

- Un Servidor de administración virtual carece de la mayoría de las configuraciones globales y sus propios puertos TCP.
- Un Servidor de administración virtual no tiene Servidores de administración secundarios.
- Un Servidor de administración virtual no tiene otros Servidores de administración virtuales.

- En un Servidor de administración físico se ven los dispositivos, grupos, eventos y objetos de los dispositivos administrados (elementos en Cuarentena, registro de aplicaciones, etc.) de todos sus Servidores de administración virtuales.
- Un Servidor de administración virtual solo puede analizar la red con puntos de distribución conectados.

## Información sobre las limitaciones de Kaspersky Security Center

La tabla siguiente muestra las limitaciones de la versión actual de Kaspersky Security Center.

Limitaciones de Kaspersky Security Center

| Tipo de limitación | Valor |
|---|---|
| Número máximo de dispositivos administrados por Servidor de administración | 100000 |
| Número máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada | 300 |
| Número máximo de grupos de administración | 10000 |
| Número máximo de eventos para almacenar | 45 000 000 |
| Número máximo de directivas | 2000 |
| Número máximo de tareas | 2000 |
| Número total máximo de objetos de Active Directory (unidades organizativas [OU] y cuentas de usuarios, dispositivos y grupos de seguridad) | 1 000 000 |
| Número máximo de perfiles en una directiva | 100 |
| Número máximo de Servidores de administración secundarios en un solo Servidor de administración principal | 500 |
| Número máximo de Servidores de administración virtual | 500 |
| Número máximo de dispositivos que un único punto de distribución puede abarcar (los puntos de distribución pueden abarcar únicamente dispositivos no móviles) | 10000 |
| Número máximo de dispositivos que pueden usar una única puerta de enlace de conexión | 10 000, incluidos los dispositivos móviles |
| Número máximo de dispositivos móviles por Servidor de administración | 100 000 menos el número de dispositivos administrados inmóviles |

## Carga de red

En esta sección, se incluye información sobre el volumen del tráfico de red que los dispositivos cliente y el Servidor de administración intercambian durante situaciones administrativas clave.

La carga principal de la red se genera a partir de los siguientes escenarios administrativos en curso:

- Despliegue inicial de la protección antivirus
- Actualización inicial de las bases de datos antivirus
- Sincronización de un dispositivo cliente con el Servidor de administración
- Actualizaciones regulares de las bases de datos antivirus
- Procesamiento de eventos en los dispositivos cliente mediante el Servidor de administración

## Despliegue inicial de la protección antivirus

Esta sección proporciona información sobre volúmenes de tráfico después de la instalación del Agente de red y Kaspersky Endpoint Security para Windows en el dispositivo cliente (consulte la siguiente tabla).

El Agente de red se instala mediante la instalación forzada, cuando el Servidor de administración copia los archivos necesarios para la instalación en una carpeta compartida en el dispositivo cliente. Después de la instalación, el Agente de red recupera el paquete de distribución de Kaspersky Endpoint Security para Windows utilizando la conexión con el Servidor de administración.

Tráfico

| Procedimiento | Instalación de Agente de red para un dispositivo cliente solo | Instalación de Kaspersky Endpoint Security para Windows en un dispositivo cliente (con bases de datos actualizadas) | Instalación simultánea del Agente de red y Kaspersky Endpoint Security para Windows |
|---|---|---|---|
| Tráfico del dispositivo cliente al Servidor de administración (KB) | 1638.4 | 7843.84 | 9707.52 |
| Tráfico del Servidor de administración al dispositivo cliente (KB) | 69,990.4 | 259,317.76 | 329,318.4 |
| Tráfico total (para un solo dispositivo cliente) (KB) | 71,628.8 | 267,161.6 | 339,025.92 |

Después de instalar Agentes de red en los dispositivos cliente, se puede asignar uno de los dispositivos del grupo de administración para que actúe como punto de distribución. Se usará para la distribución de paquetes de instalación. En este caso, el volumen de tráfico transferido durante la distribución inicial de la protección antivirus variará de manera significativa si se usa la opción de multidifusión IP.

Si se utiliza la multidifusión IP, los paquetes de instalación se envían una vez a todos los dispositivos del grupo de administración que están en funcionamiento. De esta manera, el tráfico total es N veces menor, donde N es el número total de dispositivos del grupo de administración que están en funcionamiento. Si no se usa la multidifusión IP, el tráfico total es idéntico al tráfico que se produce cuando los paquetes de distribución se descargan del Servidor de administración. Sin embargo, el origen del paquete es el punto de distribución, no el Servidor de administración.

## Actualización inicial de las bases de datos antivirus

Las tasas de tráfico durante la actualización inicial de las bases de datos antivirus (al iniciar la tarea de actualización de las bases de datos por primera vez en un dispositivo cliente) son las siguientes:

- Tráfico del dispositivo cliente al Servidor de administración: 1,8 MB.
- Tráfico del Servidor de administración al dispositivo cliente: 113 MB.
- Tráfico total (para un solo dispositivo cliente): 114 MB.

Es posible que los datos varíen levemente, según la versión actual de la base de datos antivirus.

## Sincronización de un cliente con el Servidor de administración

Este escenario describe el estado del sistema de administración cuando se produce una sincronización intensiva de datos entre un dispositivo cliente y el Servidor de administración. Los dispositivos cliente se conectan al Servidor de administración con el intervalo definido por el administrador. El Servidor de administración compara el estado de datos de un dispositivo cliente con esto en el Servidor, registra la información en la base de datos sobre la última conexión del dispositivo cliente y sincroniza datos.

Esta sección contiene información sobre los valores de tráfico de los escenarios de administración básicos que implican la conexión de un cliente con el Servidor de administración (consulte la tabla a continuación). Es posible que los datos de la tabla varíen levemente, según la versión actual de la base de datos antivirus.

| Procedimiento | Tráfico de los dispositivos cliente al Servidor de administración (KB) | Tráfico del Servidor de administración a los dispositivos cliente (KB) | Tráfico total (para un solo dispositivo cliente) (KB) |
|---|---|---|---|
| Sincronización inicial antes de actualización de bases de datos en un dispositivo cliente | 699.44 | 568.42 | 1267.86 |
| Sincronización inicial después de actualización de bases de datos en un dispositivo cliente | 735.8 | 4474.88 | 5210.68 |
| Sincronización si no hay cambios en un dispositivo cliente y el Servidor de administración | 11.99 | 6.73 | 18.72 |
| Sincronización después de cambiar el valor de una configuración en una directiva de grupo | 9.79 | 11.39 | 21.18 |
| Sincronización después de cambiar el valor de una configuración en una tarea de grupo | 11.27 | 11.72 | 22.99 |
| Sincronización forzada sin cambios en un dispositivo cliente | 77.59 | 99.45 | 177.04 |

El volumen de tráfico general varía considerablemente según si se utiliza la multidifusión IP dentro de los grupos de administración. Si la multidifusión del IP se utiliza, el volumen de tráfico total disminuye aproximadamente N veces para el grupo, donde N es el número total de dispositivos incluidos en el grupo de administración.

El volumen de tráfico en la sincronización inicial antes y después de una actualización de las bases de datos se especifica para los siguientes casos:

- Instalación del Agente de red y una aplicación de seguridad en un dispositivo cliente
- Movimiento de un dispositivo cliente a un grupo de administración
- Aplicar una directiva y tareas que se han creado para el grupo de forma predeterminada, a un dispositivo cliente

La tabla especifica los volúmenes de tráfico si se cambia una de las configuraciones de protección que se incluyen en la configuración de la Directiva de Kaspersky Endpoint Security. Los datos de otras configuraciones de la directiva pueden diferir de aquellos que se muestran en la tabla.

## Actualización adicional de las bases de datos antivirus

Las tasas de tráfico en el caso de una actualización incremental de las bases de datos antivirus 20 horas después de la actualización anterior son las siguientes:

- Tráfico del dispositivo cliente al Servidor de administración: 169 KB.
- Tráfico del Servidor de administración al dispositivo cliente: 16 MB.
- Tráfico total (para un solo dispositivo cliente): 16,3 MB.

Es posible que los datos de la tabla varíen levemente, según la versión actual de la base de datos antivirus.

El volumen de tráfico varía considerablemente si se utiliza la multidifusión IP dentro de los grupos de administración. Si la multidifusión del IP se utiliza, el volumen de tráfico total disminuye aproximadamente N veces para el grupo, donde N es el número total de dispositivos incluidos en el grupo de administración.

## Procesamiento de eventos de clientes mediante el Servidor de administración

En esta sección, se proporciona información sobre el volumen de tráfico si en un dispositivo cliente ocurre un evento "Virus detectado", que se envía al Servidor de administración y se registra en la base de datos (ver la tabla a continuación).

Tráfico

| Procedimiento | Datos transferidos al Servidor de administración después de un evento "Virus detectados" | Datos transferidos al Servidor de administración después de nueve eventos "Virus detectados" |
|---|---|---|
| Tráfico del dispositivo cliente al Servidor de administración (KB) | 49.66 | 64.05 |
| Tráfico del Servidor de administración al dispositivo cliente (KB) | 28.64 | 31.97 |
| Tráfico total (para un solo dispositivo cliente) (KB) | 78.3 | 96.02 |

Los datos de la tabla pueden variar levemente, según la versión actual de la aplicación antivirus y los eventos definidos en la directiva para el registro en la base de datos del Servidor de administración.

### Tráfico de 24 horas

Esta sección contiene la información sobre el volumen de tráfico durante 24 horas de la actividad del sistema de la administración en una condición "tranquila", cuando los dispositivos cliente o por el Servidor de administración no experimentan cambios (ver la tabla a continuación).

Los datos de la tabla describen la condición de la red después de la instalación estándar de Kaspersky Security Center y del cierre del Asistente de inicio rápido. La frecuencia de sincronización del dispositivo cliente con el Servidor de administración era de 20 minutos; las actualizaciones se descargaron al repositorio del Servidor de administración cada hora.

Tasas de tráfico por 24 horas en estado inactivo

| Flujo de tráfico | Valor |
|---|---|
| Tráfico del dispositivo cliente al Servidor de administración (KB) | 3235.84 |
| Tráfico del Servidor de administración al dispositivo cliente (KB) | 64,378.88 |
| Tráfico total (para un solo dispositivo cliente) (KB) | 67,614.72 |

## Preparación para la administración de dispositivos móviles

Esta sección proporciona la siguiente información:

- Acerca del Servidor de MDM para iOS destinado a la administración de dispositivos iOS al instalar perfiles de MDM para iOS dedicados en ellos.
- Acerca de la administración de dispositivos móviles con Kaspersky Endpoint Security para Android instalado.

## Servidor de MDM para iOS

El Servidor de MDM para iOS le permite administrar dispositivos iOS al instalar perfiles de MDM para iOS dedicados en ellos. Las funciones siguientes se admiten:

- Bloqueo del dispositivo
- Restablecimiento de contraseña
- Eliminación de datos
- Instalación o eliminación de aplicaciones
- Uso de un perfil de MDM para iOS con configuración avanzada (por ejemplo configuración de VPN, configuración del correo electrónico, configuración de Wi-Fi, configuración de la cámara, certificados, etc.)

El Servidor de MDM para iOS es un servicio web que recibe conexiones entrantes de dispositivos móviles a través de su puerto TLS (de forma predeterminada, puerto 443), que es administrado por Kaspersky Security Center mediante el Agente de red. El Agente de red se instala localmente en un dispositivo que tiene también instalado un Servidor de MDM para iOS.

Al instalar un Servidor de MDM para iOS, el administrador debe realizar las siguientes acciones:

- Proporcionar acceso al Servidor de administración al Agente de red
- Proporcionar acceso al puerto TCP del Servidor de MDM para iOS a los dispositivos móviles

Esta sección está dirigida a dos configuraciones estándares de un Servidor de MDM para iOS.

### Configuración estándar: Kaspersky Device Management for iOS en una DMZ

Un Servidor de MDM para iOS se localiza en la DMZ de la red local de una organización con acceso a Internet. Una característica especial de este enfoque es la ausencia de cualquier problema cuando al servicio web de MDM para iOS se accede desde dispositivos a través de Internet.

Como la administración de un Servidor de MDM para iOS requiere un Agente de red para instalarlo localmente, debe asegurar la interacción del Agente de red con el Servidor de administración. Puede garantizarlo usando uno de los siguientes métodos:

- Desplazando el Servidor de administración a la DMZ.
- Usando una puerta de enlace de conexión:

  a. En el dispositivo en el que se haya instalado el Servidor de MDM para iOS, conecte el Agente de red al Servidor de administración a través de una puerta de enlace de conexión.

  b. En el dispositivo en el que se haya instalado el Servidor de MDM para iOS, asigne un Agente de red para que actúe como puerta de enlace de conexión.

### Configuración estándar: Servidor de MDM para iOS en la red local de una organización

Un Servidor de MDM para iOS se localiza en la red interna de una organización. El puerto 443 (puerto predeterminado) debe habilitarse para el acceso externo, por ejemplo, publicando el servicio web de MDM para iOS en el proxy inverso compatible con la delegación restringida de Kerberos.

Cualquier configuración estándar requiere acceso a servicios web de Apple para el Servidor de MDM para iOS (rango 17.0.0.0/8) a través del puerto TCP 2197. Este puerto se utiliza para notificar a los dispositivos sobre nuevos comandos por medio de un servicio dedicado llamado APNs.

### Administración de dispositivos móviles con Kaspersky Endpoint Security para Android

Los dispositivos móviles con Kaspersky Endpoint Security para Android™ instalado (denominados, en lo sucesivo, dispositivos KES) se administran por medio del Servidor de administración. Kaspersky Security Center admite las siguientes funciones para administrar dispositivos KES:

- Manejo de dispositivos móviles como dispositivos cliente:
  - Membrecía en grupos de administración
  - Supervisión, por ejemplo, ver estados, eventos e informes
  - Modificación de la configuración local y asignación de directivas para Kaspersky Endpoint Security para Android
- Envío de comandos en modo centralizado
- Instalación de paquetes de aplicaciones móviles remotamente

El Servidor de administración administra los dispositivos KES mediante TLS, puerto TCP 13292.

## Información sobre el rendimiento del Servidor de administración

Esta sección presenta los resultados de las pruebas de rendimiento del Servidor de administración para diferentes configuraciones de hardware, así como las limitaciones para conectar dispositivos administrados al Servidor de administración.

### Limitaciones en la conexión a un Servidor de administración

Un Servidor de administración admite la administración de hasta 100000 dispositivos sin una pérdida en el rendimiento.

Limitaciones de conexiones con un Servidor de administración sin una pérdida de rendimiento:

- Un Servidor de administración puede admitir hasta 500 Servidores de administración virtuales.
- El Servidor de administración principal no admite más que 1000 sesiones simultáneamente.
- Los Servidores de administración virtuales no admiten más que 1000 sesiones simultáneamente.

## Resultados de las pruebas de rendimiento del Servidor de administración

Los resultados de las pruebas de rendimiento del Servidor de administración nos han permitido determinar los números máximos de dispositivos cliente con las cuales se puede sincronizar el Servidor de administración dentro de los períodos especificados. Puede utilizar esta información para seleccionar el esquema óptimo para instalar la protección antivirus en redes de dispositivos.

Para realizar pruebas, se utilizaron dispositivos con las siguientes configuraciones de hardware (consulte las tablas a continuación):

Configuración de hardware del Servidor de administración

| Parámetro | Valor |
|---|---|
| CPU | Intel Xeon CPU E5630, velocidad del reloj de 2.53 GHz, 2 socket, 8 núcleos, 16 procesadores lógicos |
| RAM | 26 GB |
| Disco duro | Dispositivo de disco IBM ServeRAID M5014 SCSI, 487 GB |
| Sistema operativo | Microsoft Windows Server 2019 Standard, versión 10.0.17763, compilación 17763 |
| Red | QLogic BCM5709C Gigabit Ethernet (NDIS VBD Client) |

Configuración de hardware del dispositivo del Servidor SQL

| Parámetro | Valor |
|---|---|
| CPU | Intel Xeon CPU X5570, velocidad del reloj de 2.93 GHz, 2 socket, 8 núcleos, 16 procesadores lógicos |
| RAM | 32 GB |
| Disco duro | Adaptec Array SCSI Disk Device, 2047 GB |
| Sistema operativo | Microsoft Windows Server 2019 Standard, versión 10.0.17763, compilación 17763 |
| Red | Intel 82576 Gigabit |

El Servidor de administración colaboró con la creación de 500 Servidores de administración virtuales.

El intervalo de sincronización era de 15 minutos por cada 10000 dispositivos administrados (consulte la siguiente tabla).

Resultados resumidos de la prueba de la carga del Servidor de administración

| Intervalo de sincronización (min.) | Número de dispositivos administrados |
|---|---|
| 15 | 10000 |
| 30 | 20000 |
| 45 | 30000 |
| 60 | 40000 |
| 75 | 50000 |
| 90 | 60000 |
| 105 | 70000 |
| 120 | 80000 |

| Intervalo de sincronización (min.) | Número de dispositivos administrados |
|---|---|
| 135 | 90000 |
| 150 | 100000 |

Si conecta el Servidor de administración a un servidor de bases de datos MySQL o SQL Express, recomendamos que no administre más de 10000 dispositivos con la aplicación. Para el servidor de bases de datos MariaDB, el máximo recomendado es de 20000 dispositivos administrados.

## Resultados de las pruebas de rendimiento del servidor Proxy de KSN

Si la red de su empresa incluye una gran cantidad de dispositivos cliente y utilizan el Servidor de administración como servidor proxy de KSN, el hardware del Servidor de administración debe cumplir requisitos específicos para poder procesar las solicitudes de los dispositivos cliente. Puede usar los resultados de las pruebas a continuación para evaluar la carga del Servidor de administración en su red y planificar los recursos de hardware para proporcionar el funcionamiento normal del servicio del proxy de KSN.

Las tablas siguientes muestran la configuración de hardware del Servidor de administración y SQL Server. Esta configuración se utilizó para realizar pruebas.

Configuración de hardware del Servidor de administración

| Parámetro | Valor |
|---|---|
| CPU | Intel Xeon CPU E5450, velocidad del reloj de 3.00 GHz, 2 sockets, 8 núcleos, 16 procesadores lógicos |
| RAM | 32 GB |
| Sistema operativo | Microsoft Windows Server 2016 Standard |

Configuración de hardware de SQL Server

| Parámetro | Valor |
|---|---|
| CPU | Intel Xeon CPU E5450, velocidad del reloj de 3.00 GHz, 2 sockets, 8 núcleos, 16 procesadores lógicos |
| RAM | 32 GB |
| Sistema operativo | Microsoft Windows Server 2019 Standard |

La siguiente tabla muestra los resultados de la prueba.

Resultados resumidos de pruebas de rendimiento del servidor proxy de KSN

| Parámetro | Valor |
|---|---|
| Número máximo de solicitudes procesadas por segundo | 4914 |
| Utilización máxima de la CPU | 36% |

# Configuración de la red para interactuar con servicios externos

Kaspersky Security Center utiliza la siguiente configuración de red para interactuar con servicios externos.

| Configuración de red | Dirección | Descripción |
|---|---|---|
| Puerto: 443<br>Protocolo: HTTPS | activación-v2.kaspersky.com | Activación de la aplicación. |
| Puerto: 443<br>Protocolo: HTTPS | https://s00.upd.kaspersky.com<br>https://s01.upd.kaspersky.com<br>https://s02.upd.kaspersky.com<br>https://s03.upd.kaspersky. com<br>https://s04.upd.kaspersky.com<br>https://s05.upd.kaspersky.com<br>https://s06.upd.kaspersky.com<br>https://s07.upd.kaspersky.com<br>https: // s08 .upd.kaspersky.com<br>https://s09.upd.kaspersky.com<br>https://s10.upd.kaspersky.com<br>https://s11.upd.kaspersky.com<br>https://s12.upd.kaspersky.com<br>https://s13.upd.kaspersky.com<br>https://s14.upd.kaspersky.com<br>https://s15.upd.kaspersky.com<br>https://s16.upd.kaspersky.com<br>https: // s17. upd.kaspersky.com<br>https://s18.upd.kaspersky.com<br>https://s19.upd.kaspersky.com<br>https://cm.k.kaspersky-labs.com | Actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky. |
| Puerto: 443<br>Protocolo: HTTPS | https://downloads.upd.kaspersky.com | • Actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky.<br>• Comprobar si se puede acceder a los servidores de Kaspersky.<br>Antes de descargar las bases de datos y los módulos de software de Kaspersky, Kaspersky Security Center verifica que haya acceso a los servidores de Kaspersky. Si los servidores DNS configurados en el sistema no permiten acceder a los servidores de Kaspersky, la aplicación utiliza servidores DNS públicos. |

| Configuración de red | Dirección | Descripción |
| --- | --- | --- |
| Puerto: 80<br>Protocolo: HTTP | http://p00.upd.kaspersky.com<br>http://p01.upd.kaspersky.com<br>http : //p02.upd.kaspersky.com<br>http://p03.upd.kaspersky.com<br>http://p04.upd.kaspersky.com<br>http://p05.upd.kaspersky.com<br>http: //p06.upd .kaspersky.com<br>http://p07.upd.kaspersky.com<br>http://p08.upd.kaspersky.com<br>http://p09.upd.kaspersky.com<br>http://p10.upd.kaspersky.com<br>http: //p11.upd.kaspersky.com<br>http: //p12.upd.kaspersky .com<br>http://p13.upd.kaspersky.com<br>http://p14.upd.kaspersky.com<br>http://p15.upd.kaspersky.com<br>http://p16.upd.kaspersky.com<br>http: // p17.upd.kaspersky.com<br>http://p18.upd.kaspersky.com<br>http://p19.upd.kaspersky.com<br>http://downloads0.kaspersky-labs.com<br>http://downloads1.kaspersky-labs.com<br>http://downloads2.kaspersky-labs.com<br>http://downloads3.kaspersky-labs.com<br>http://downloads4.kaspersky-labs.com<br>http://downloads5.kaspersky-labs.com<br>http://downloads6.kaspersky-labs.com<br>http://downloads7.kaspersky-labs.com<br>http://downloads8.kaspersky-labs.com<br>http://downloads9.kaspersky-labs.com<br>http://downloads.kaspersky-labs.com<br>http://cm.k.kaspersky-labs.com | Actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky. |
| Puerto: 443<br>Protocolo: HTTPS | ds.kaspersky.com<br>dc1.ksn.kaspersky-labs.com<br>dc1-file.ksn.kaspersky-labs.com<br>dc1-pp.ksn.kaspersky-labs.com<br>dc1-st.ksn.kaspersky-labs.com | Usar Kaspersky Security Network. |
| Puerto: 443, 1443<br>Protocolo: HTTPS | ksn-file-geo.kaspersky-labs.com<br>ksn-verdict-geo.kaspersky-labs.com<br>ksn-url-geo.kaspersky-labs.com<br>ksn-a-p2p-geo.kaspersky-labs.com<br>ksn-info-geo.kaspersky-labs.com<br>ksn-cinfo-geo.kaspersky-labs.com | Usar Kaspersky Security Network. |
| Puerto: 443<br>Protocolo: HTTPS | click.kaspersky.com<br>redirect.kaspersky.com | Seguir los enlaces desde la interfaz. |

| Configuración de red | Dirección | Descripción |
|---|---|---|
| Puerto: 80<br>Protocolo: HTTP | http://crl.kaspersky.com<br>http://ocsp.kaspersky.com | Estos servidores forman parte de la Infraestructura de clave pública (PKI) y son necesarios para verificar el estado de validez de los certificados de firma digital de Kaspersky. La CRL es una lista de certificados revocados. El OCSP le permite solicitar el estado de un certificado específico en tiempo real. Estos servidores ayudan a garantizar la seguridad de la interacción con certificados digitales y protegen contra posibles ataques. |
| Puerto: 443<br>Protocolo: HTTPS | https://ipm-klca.kaspersky.com | Novedades con fines publicitarios. |

Para una interacción adecuada de Kaspersky Security Center con servicios externos, considere las siguientes recomendaciones:
Se debe permitir el tráfico de red no cifrado en los puertos 443 y 1443 del equipo de red y del servidor proxy de su organización.
Cuando el Servidor de administración interactúa con los servidores de actualización de Kaspersky y los servidores de Kaspersky Security Network, es necesario evitar el secuestro del tráfico de red con sustitución de certificados (ataques de MITM).

*Para descargar actualizaciones a través del protocolo HTTP o HTTPS utilizando la utilidad klscflag:*

1. Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada es <Disk>:\Archivos de programa(x86)\Kaspersky Lab\Kaspersky Security Center.

2. Si desea descargar actualizaciones a través del protocolo HTTP, ejecute uno de los siguientes comandos:

   - En el dispositivo en el que se encuentra instalado el Servidor de administración:

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - En un punto de distribución:

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   Si desea descargar actualizaciones a través del protocolo HTTPS, ejecute uno de los siguientes comandos:

   - En el dispositivo en el que se encuentra instalado el Servidor de administración:

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - En un punto de distribución:

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

# Despliegue del Agente de red y de la aplicación de seguridad

Para administrar dispositivos en una organización, tiene que instalar el Agente de red en cada uno de ellos. La distribución de Kaspersky Security Center distribuido en dispositivos corporativos normalmente comienza con la instalación del Agente de red en ellos.

En Microsoft Windows XP, el Agente de red podría no realizar las siguientes operaciones correctamente: descargar actualizaciones directamente desde los servidores de Kaspersky (como un punto de distribución); funcionar como servidor proxy de KSN (como un punto de distribución); detectar vulnerabilidades de terceros (si se usa la Administración de vulnerabilidades y parches).

## Despliegue inicial

Para administrar dispositivos en una organización, tiene que instalar el Agente de red en cada uno de ellos.

La instalación del Agente de red en el dispositivo administrado que ejecuta Windows se puede realizar de las siguientes maneras:

- Con herramientas de terceros para la instalación remota de aplicaciones.
- Mediante la clonación de una imagen del disco duro del administrador con el sistema operativo y el Agente de red: usando herramientas proporcionadas por Kaspersky Security Center para gestionar imágenes del disco o usando herramientas de terceros.
- Mediante directivas de grupo de Windows: usando herramientas estándares de administración de Windows para directivas de grupo, o en modo automático, a través de la opción correspondiente dedicada en la tarea de instalación remota de Kaspersky Security Center.
- En modo forzado, utilizando los recursos del sistema operativo a través de la tarea de instalación remota de Kaspersky Security Center.
- Al enviar vínculos de usuarios del dispositivo a paquetes independientes generados por Kaspersky Security Center. Los paquetes independientes son módulos ejecutables que contienen los paquetes de distribución de aplicaciones seleccionadas con su configuración definida.
- Manualmente, mediante la ejecución de instaladores de la aplicación en los dispositivos.

La instalación inicial del Agente de red en el dispositivo administrado que ejecuta Linux se puede realizar de las siguientes maneras:

- Conectarse al dispositivo administrado a través de SSH y ejecutar la tarea de instalación remota.
- Ejecutar el paquete de instalación en el dispositivo administrado.

La instalación inicial del Agente de red en el dispositivo administrado que ejecuta macOS se puede realizar de las siguientes maneras:

- Ejecutar la tarea de instalación remota a través del punto de distribución de macOS.
- Al enviar vínculos de usuarios del dispositivo a paquetes independientes generados por Kaspersky Security Center. Los paquetes independientes son módulos ejecutables que contienen los paquetes de distribución de aplicaciones seleccionadas con configuración predefinida.

Después de que se instala el Agente de red en un dispositivo, puede realizar la instalación remota de las aplicaciones de Kaspersky en ese dispositivo a través de este Agente de red. El paquete de distribución de una aplicación que se debe instalar se transfiere a través de canales de comunicación entre Agentes de red y el Servidor de administración, junto con la configuración de instalación definida por el administrador. Para transferir el paquete de distribución, puede usar nodos de distribución de relevo, es decir puntos de distribución, distribución multidifusión, etc.

Al seleccionar un método y una estrategia para desplegar las aplicaciones en una red administrada, debe considerar varios factores (lista parcial):

- Configuración de red de la organización.
- Número total de dispositivos.
- Presencia de dispositivos en la red de la organización, que no son miembros de ningún dominio de Active Directory, y la presencia de cuentas uniformes con derechos de administrador en esos dispositivos.
- Capacidad del canal entre el Servidor de administración y los dispositivos.
- Tipo de comunicación entre el Servidor de administración y subredes remotas y la capacidad de los canales de la red en esas subredes.
- Configuración de seguridad aplicada en dispositivos remotos al inicio del despliegue. Estos parámetros permiten establecer la conexión remota al dispositivo administrado e iniciar la instalación.

## Configuración de instaladores

Antes de desplegar las aplicaciones de Kaspersky en una red, debe especificar la configuración de instalación, es decir, los parámetros que se configuran durante la instalación de la aplicación. Al instalar el Agente de red, debería especificar, como mínimo, una dirección para la conexión con el Servidor de administración. Es posible que también se soliciten algunas configuraciones avanzadas. Según el método de instalación que haya seleccionado, puede definir la configuración de varias formas. En el caso más sencillo (instalación interactiva manual en un dispositivo seleccionado), toda la configuración relevante se puede definir a través de la interfaz de usuario del instalador.

Este método para definir la configuración es inadecuado para la instalación no interactiva ("silenciosa") de aplicaciones en grupos de dispositivos. En un caso típico, el administrador debe indicar de forma centralizada los valores de los parámetros, que luego pueden usarse para la instalación no interactiva en los dispositivos de red seleccionados.

## Paquetes de instalación

El primer método y el principal de definición de la configuración de instalación de aplicaciones es de uso múltiple y, por consiguiente, conveniente para todos los métodos de instalación, tanto con herramientas de Kaspersky Security Center como con la mayor parte de herramientas de terceros. Este método consiste en crear paquetes de instalación de aplicaciones en Kaspersky Security Center.

Los paquetes de instalación se generan usando los métodos siguientes:

- Automáticamente, desde paquetes de distribución especificados, sobre la base de *descriptores* incluidos (archivos con la extensión kud que contienen reglas para instalación y análisis de resultados y otra información).

- Utilizando los archivos ejecutables de los instaladores o utilizando instaladores en formatos nativos (.msi, .deb o .rpm), para aplicaciones estándar o compatibles.

Los paquetes de instalación generados se organizan jerárquicamente como carpetas, con subcarpetas y archivos. Además del paquete de distribución original, un paquete de instalación contiene la configuración editable (incluida la configuración del instalador y reglas para procesar tales casos como la necesidad de reiniciar el sistema operativo a fin de completar la instalación), así como los módulos auxiliares menores.

Los valores de la configuración de instalación específicos para una aplicación individual compatible se pueden definir en la interfaz de usuario de la Consola de administración, durante la creación del paquete de instalación. Al realizar la instalación remota de aplicaciones a través de herramientas de Kaspersky Security Center, los paquetes de instalación se entregan a dispositivos de modo que, si se ejecuta el instalador de una aplicación, toda la configuración definida por los administradores quede a disposición para esa aplicación. Al usar herramientas de terceros para la instalación de aplicaciones de Kaspersky, solo tiene que asegurar la disponibilidad del paquete de instalación completo en el dispositivo; es decir, la disponibilidad del paquete de distribución y su configuración. Los paquetes de instalación se crean y almacenan mediante Kaspersky Security Center en una subcarpeta dedicada de la carpeta compartida.

No especifique ningún detalle de cuentas privilegiadas en los parámetros de los paquetes de instalación.

Para obtener instrucciones sobre el uso de este método de configuración de las aplicaciones de Kaspersky antes de instalarlas a través de herramientas de terceros, consulte la sección Despliegue mediante directivas de grupo de Microsoft Windows.

Inmediatamente después de la instalación de Kaspersky Security Center, unos paquetes de instalación se generan automáticamente; están listos para la instalación e incluyen paquetes del Agente de red y paquetes de aplicaciones de seguridad para Microsoft Windows.

A pesar de que la clave de licencia para la licencia de la aplicación se puede establecer en las propiedades del paquete de instalación, no es aconsejable utilizar este método de distribución de licencias debido a que es fácil obtener acceso de lectura a los paquetes de instalación. Lo que hay que hacer es usar claves de licencia de distribución automática o tareas de instalación de claves de licencia.

## Propiedades MSI y archivos de transformación

Otro modo de configurar la instalación en la plataforma de Windows es definir propiedades MSI y archivos de transformación. Este método se puede aplicar en los casos siguientes:

- Al realizar la instalación mediante las Directivas de grupo de Windows utilizando herramientas regulares de Microsoft u otras herramientas de terceros para trabajar con Directivas de grupo de Windows.

- Al instalar aplicaciones usando herramientas de terceros destinadas al trabajo con instaladores en el formato de Microsoft Installer.

## Despliegue con herramientas de terceros para la instalación remota de aplicaciones

Si en la organización se cuenta con herramientas para la instalación remota de aplicaciones (por ejemplo Microsoft System Center), es conveniente realizar el despliegue inicial con esas herramientas.

Se deben ejecutar las siguientes acciones:

- Seleccionar el método para configurar la instalación que se adapte mejor a la herramienta de despliegue que se utilizará.
- Definir el mecanismo de sincronización entre la modificación de la configuración de paquetes de instalación (a través de la interfaz de la Consola de administración) y la operación de determinadas herramientas de terceros usadas para el despliegue de aplicaciones a partir de los datos del paquete de instalación.
- Al realizar la instalación desde una carpeta compartida, se debe asegurar de que este recurso de archivos tenga la capacidad suficiente.

## Acerca de las tareas de instalación remota en Kaspersky Security Center

Kaspersky Security Center proporciona varios mecanismos para la instalación remota de aplicaciones, que se implementan como tareas de instalación remotas (instalación forzada, instalación al copiar una imagen del disco duro, instalación a través de directivas de grupo de Microsoft Windows). Puede crear una tarea de instalación remota tanto para un grupo de administración especificado como para dispositivos específicos o una selección de dispositivos (tales tareas se muestran en la Consola de administración, en la carpeta **Tareas**). Al crear una tarea, puede seleccionar paquetes de instalación (los del Agente de red u otra aplicación) que se instalarán dentro de esta tarea, así como especificar ciertas configuraciones que definan el método de la instalación remota. Además, puede usar el Asistente de instalación remota, que se basa en la creación de una tarea de instalación remota y da como resultado la supervisión.

Las Tareas para grupos de administración afectan a ambos dispositivos incluidos en un grupo especificado y todos los dispositivos en todos los subgrupos dentro de ese grupo de administración. Una tarea cubre dispositivos de Servidores de administración secundarios incluidos en un grupo o cualquiera de sus subgrupos si la configuración correspondiente se habilita en la tarea.

Las tareas para dispositivos específicos actualizan la lista de dispositivos cliente en cada ejecución de acuerdo con el contenido de la selección en el momento en el que se inicia la tarea. Si una selección incluye dispositivos que se han conectado a Servidores de administración secundarios, la tarea también se ejecutará en esos dispositivos. Para obtener más información sobre esas configuraciones y métodos de instalación, consulte la siguiente información en esta sección.

Para asegurar la operación correcta de una tarea de instalación remota en dispositivos conectados a Servidores de administración secundarios, debe usar la tarea de retransmisión para retransmitir paquetes de instalación usados por su tarea a los Servidores de administración secundarios correspondientes de antemano.

## Despliegue mediante la captura y copia de la imagen de un dispositivo

Si tiene que instalar el Agente de red en dispositivos en los cuales un sistema operativo y otro software también se deben instalar (o volver a instalar), puede usar el mecanismo de captura y copia de la imagen de ese dispositivo.

*Para realizar un despliegue con una imagen de disco duro:*

1. Cree un dispositivo de referencia con un sistema operativo y el software relevante instalado, incluidos el Agente de red y una aplicación de seguridad.

2. Capture la imagen de la referencia en el dispositivo y distribuya esa imagen en dispositivos nuevos a través de la tarea dedicada de Kaspersky Security Center.

   Para capturar e instalar imágenes de disco, puede usar herramientas de terceros disponibles en la organización o la función proporcionada (según una licencia de Administración de vulnerabilidades y parches) mediante Kaspersky Security Center.

Si usa algunas herramientas de terceros para procesar las imágenes del disco, debe eliminar las información que usa Kaspersky Security Center para identificar el dispositivo administrado, al realizar la distribución en un dispositivo desde una imagen de referencia. De otra forma, el Servidor de administración no podrá distinguir correctamente los dispositivos que se han creado al copiar la misma imagen.

Al capturar una imagen de disco con herramientas de Kaspersky Security Center, este problema se soluciona automáticamente.

## Copia de una imagen de disco con herramientas de terceros

Al aplicar herramientas de terceros para capturar la imagen de un dispositivo con el Agente de red instalado, use uno de los métodos siguientes:

- Método recomendado. Al instalar el Agente de red en un dispositivo de referencia, capture la imagen del dispositivo antes de la primera ejecución del servicio del Agente de red (porque los datos exclusivos que identifican el dispositivo se crean en la primera conexión del Agente de red con el Servidor de administración). Después de esto, se recomienda que evite ejecutar el servicio del Agente de red hasta la finalización de la operación de captura de la imagen.

- En el dispositivo de referencia, detenga el servicio del Agente de red y ejecute la utilidad klmover con la clave -dupfix. La utilidad klmover se incluye en el paquete de instalación del Agente de red. Evite cualquier ejecución subsiguiente del servicio del Agente de red hasta que la operación de captura de la imagen se complete.

- Asegúrese de que klmover se ejecute con la clave -dupfix antes (requisito obligatorio) de la primera ejecución del servicio del Agente de red en dispositivos de destino, en el primer inicio del sistema operativo después del despliegue de la imagen. La utilidad klmover se incluye en el paquete de instalación del Agente de red.

- Utilice el modo de clonación de disco del Agente de red.

Si la imagen del disco duro no se copió correctamente, existen métodos para resolver el problema.

También puede capturar la imagen de un dispositivo sin el Agente de red instalado. Para hacerlo, realice el despliegue de la imagen en los dispositivos de destino y luego despliegue el Agente de red. Si utiliza este método, proporcione acceso a la carpeta de red con paquetes de instalación independientes desde un dispositivo.

## Copia incorrecta de una imagen del disco duro

Cuando una imagen de disco duro con el Agente de red instalado se copia sin seguir las reglas de despliegue, puede suceder que varios dispositivos aparezcan juntos en la Consola de administración, con un mismo ícono y un nombre que cambia constantemente.

Puede resolver este problema usando uno de los siguientes métodos:

- Eliminando el Agente de red

  Este método es el más fiable. Debe eliminar el Agente de red en dispositivos que se hayan copiado incorrectamente de la imagen, usando herramientas de terceros y, luego, volver a instalarlo. El Agente de red no se puede eliminar a través de las herramientas de Kaspersky Security Center, porque el Servidor de administración no puede distinguir entre dispositivos defectuosos (todos ellos comparten el mismo icono en la Consola de administración).

- Ejecución de la utilidad klmover con la clave "-dupfix"

  En los dispositivos con problemas (aquellos que se copiaron incorrectamente de la imagen) es necesario usar herramientas de terceros para ejecutar una vez la utilidad klmover, ubicada en la carpeta de instalación del Agente de Administración con el modificador "-dupfix" (klmover -dupfix). No es posible ejecutar la utilidad con Kaspersky Security Center, porque el Servidor de administración no puede distinguir entre dispositivos defectuosos (todos comparten el mismo icono en la Consola de administración).

  A continuación, elimine el icono en el cual se habían mostrado los dispositivos defectuosos antes de ejecutar la herramienta.

- Endurecimiento de la regla para la detección de dispositivos copiados incorrectamente.

  > Este método solo es aplicable si están instalados el Servidor de administración y Agente de red versión 10 Service Pack 1 o posteriores.

  La regla para la detección de Agentes de red copiados incorrectamente se debe endurecer para que el cambio del nombre NetBIOS de un dispositivo resulte en una "solución" automática de esos Agentes de red (suponiendo que todos los dispositivos copiados tienen nombres NetBIOS únicos).

  En el dispositivo con el Servidor de administración, debe importar el archivo de registro mostrado a continuación al Registro y luego reiniciar el servicio del Servidor de administración.

  - Si hay un sistema operativo de 32 bits instalado en el dispositivo del Servidor de administración:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

  - Si un sistema operativo de 64 bits está instalado en el dispositivo con el Servidor de administración:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

## Despliegue mediante directivas de grupo de Microsoft Windows

Se recomienda que realice el despliegue inicial del Agente de red a través de directivas de grupo de Microsoft Windows si las condiciones siguientes se cumplen:

- El dispositivo es miembro de un dominio de Active Directory.
- El esquema de despliegue permite esperar al siguiente reinicio de rutina de los dispositivos de destino antes de comenzar a instalar el Agente de red en ellos (o puede forzar la aplicación de una directiva de grupo de Windows en esos dispositivos).

Este esquema de despliegue consiste en lo siguiente:

- El paquete de distribución de aplicaciones en el formato de Microsoft Installer (paquete MSI) se localiza en una carpeta compartida (una carpeta donde las cuentas de LocalSystem de dispositivos de destino tienen permisos de lectura).
- En la directiva de grupo de Active Directory, un objeto de instalación se crea para el paquete de distribución.
- El alcance de instalación está configurado al especificar la unidad organizativa (OU) o el grupo de seguridad, que incluye los dispositivos de destino.
- La próxima vez que un dispositivo de destino inicia sesión en el dominio (antes de que los usuarios del dispositivo inicien sesión en el sistema), todas las aplicaciones instaladas se examinan para ver la presencia de la aplicación requerida. Si la aplicación no se encuentra, el paquete de distribución se descarga desde el recurso especificado en la directiva y se instala a continuación.

Una ventaja de este esquema de despliegue consiste en que las aplicaciones asignadas se instalan en los dispositivos de destino mientras el sistema operativo se está cargando, es decir, incluso antes de que el usuario inicie sesión en el sistema. Aun si un usuario con derechos suficientes elimina la aplicación, se instalará de nuevo en el siguiente inicio del sistema operativo. El defecto de este esquema de despliegue es que los cambios hechos por el administrador a la directiva de grupo no entrarán en vigor hasta que los dispositivos se reinicien (si no se usa ninguna herramienta adicional).

Puede usar directivas de grupo para instalar tanto el Agente de red como otras aplicaciones si sus instaladores respectivos están en el formato de Windows Installer.

Cuando este esquema de despliegue se selecciona, también debe evaluar la carga en el recurso del archivo del cual los archivos se copiarán a dispositivos después de aplicar la directiva de grupo de Windows.

## Manipulación de directivas de Microsoft Windows a través de la tarea de instalación remota de Kaspersky Security Center

La manera más sencilla de instalar aplicaciones a través de directivas de grupo de Microsoft Windows es seleccionar la opción **Asignar la instalación del paquete en las directivas de grupo de Active Directory** en las propiedades de la tarea de instalación remota de Kaspersky Security Center. En este caso, el Servidor de administración automáticamente realiza las siguientes acciones cuando ejecuta la tarea:

- Crea los objetos requeridos en la directiva de grupo de Microsoft Windows.
- Crea grupos de seguridad dedicados, incluye los dispositivos de destino en esos grupos y asigna la instalación de aplicaciones seleccionadas para ellos. El conjunto de grupos de seguridad se actualizará en cada ejecución de la tarea, de acuerdo con el grupo de dispositivos en el momento de la ejecución.

Para hacer esta función operable, en las propiedades de la tarea, especifique una cuenta que tenga permisos de escritura en las directivas de grupo de Active Directory.

Si tiene la intención de instalar tanto el Agente de red como otra aplicación a través de la misma tarea, si selecciona la opción **Asignar la instalación del paquete en las directivas de grupo de Active Directory**, la aplicación crea un objeto de instalación en la directiva de Active Directory para el Agente de red únicamente. La segunda aplicación seleccionada en la tarea se instalará a través de las herramientas del Agente de red tan pronto como este se instale en el dispositivo. Si desea instalar una aplicación además del Agente de red a través de directivas de grupo de Windows, debe crear una tarea de instalación para este paquete de instalación únicamente (sin el paquete del Agente de red). No todas las aplicaciones pueden instalarse usando directivas de grupo de Microsoft Windows. Para obtener más información sobre esta capacidad, puede consultar la información sobre los métodos posibles para instalar la aplicación.

Si los objetos necesarios se crean en la directiva de grupo usando herramientas de Kaspersky Security Center, la carpeta compartida de Kaspersky Security Center se utilizará como fuente del paquete de instalación. Al planear el despliegue, debe correlacionar la velocidad de lectura para esta carpeta con el número de dispositivos y el tamaño del paquete de distribución que se instalará. Puede ser útil localizar la carpeta compartida de Kaspersky Security Center en un repositorio de archivos dedicado de alto rendimiento.

Además de su facilidad del uso, la creación automática de directivas de grupo de Windows a través de Kaspersky Security Center tiene esta ventaja: al planear la instalación del Agente de red, puede especificar fácilmente el grupo de administración de Kaspersky Security Center en al cual los dispositivos se moverán automáticamente después de que la instalación se complete. Puede especificar este grupo en el Asistente para crear nueva tarea o en la ventana de configuración de la tarea de instalación remota.

Al gestionar directivas de grupo de Windows a través de Kaspersky Security Center, puede especificar dispositivos para un objeto de la directiva de grupo al crear un grupo de seguridad. Kaspersky Security Center sincroniza los contenidos del grupo de seguridad con el conjunto actual de dispositivos en la tarea. Al usar otras herramientas para administrar las directivas de grupo, puede asociar objetos de directivas de grupo con OU seleccionadas de Active Directory directamente.

## Instalación no asistida de aplicaciones a través de directivas de Microsoft Windows

El administrador puede crear objetos requeridos para la instalación en una directiva de grupo de Windows en su propio nombre. En este caso, él o ella pueden proporcionar vínculos a paquetes almacenados en la carpeta compartida de Kaspersky Security Center o cargar esos paquetes a un servidor de archivos dedicado y luego proporcionar vínculos a ellos.

Las situaciones de instalación siguientes son posibles:

- El administrador crea un paquete de instalación y configura sus propiedades en la Consola de administración. El objeto de la directiva de grupo proporciona un vínculo al archivo MSI de este paquete almacenado en la carpeta compartida de Kaspersky Security Center.

- El administrador crea un paquete de instalación y configura sus propiedades en la Consola de administración. A continuación, el administrador copia la subcarpeta EXEC completa de este paquete desde la carpeta compartida de Kaspersky Security Center a una carpeta en un recurso del archivo dedicado de la organización. El objeto de la directiva de grupo proporciona un enlace al archivo MSI de este paquete almacenado en la subcarpeta del recurso del archivo dedicado de la organización.

- El administrador descarga el paquete de distribución de aplicaciones (incluyendo el del Agente de red) de Internet y lo carga en el recurso del archivo dedicado de la organización. El objeto de la directiva de grupo proporciona un enlace al archivo MSI de este paquete almacenado en la subcarpeta del recurso del archivo dedicado de la organización. La configuración de instalación se define al configurar las propiedades MSI o al configurar los archivos de transformación MST.

## Despliegue forzado con la tarea de instalación remota de Kaspersky Security Center

Para desplegar por primera vez el Agente de red u otras aplicaciones, puede forzar la instalación de los paquetes de instalación seleccionados con la tarea de instalación remota de Kaspersky Security Center, siempre que cada dispositivo tenga una cuenta de usuario con derechos de administrador local.

La instalación forzada también se puede usar si no se puede acceder directamente a los dispositivos mediante el Servidor de administración: por ejemplo, los dispositivos están en redes aisladas o están en una red local mientras que el elemento del Servidor de administración está en la DMZ.

En el primer despliegue, el Agente de red no está instalado. Por lo tanto, en la configuración de la tarea de instalación remota, no se puede seleccionar la distribución de los archivos necesarios para la instalación de la aplicación mediante el Agente de red. Solo puede optar por distribuir archivos con recursos del sistema operativo a través del Servidor de administración o puntos de distribución.

El servicio del Servidor de administración debe ejecutarse bajo una cuenta que tenga privilegios administrativos en los dispositivos de destino. También puede especificar una cuenta que tenga acceso al recurso compartido admin$ en la configuración de la tarea de instalación remota.

> De manera predeterminada, la tarea de instalación remota se aplica a los dispositivos con las credenciales de la cuenta que se usa para ejecutar el Servidor de administración. Es importante aclarar que se trata de la cuenta utilizada para acceder al recurso compartido admin$, en lugar de la cuenta que se usa para ejecutar la tarea de instalación remota. La instalación se realiza con la Cuenta LocalSystem.

Puede especificar dispositivos de destino explícitamente (con una lista), mediante la selección del grupo de administración de Kaspersky Security Center al cual pertenecen o tras crear una selección de dispositivos en función de un criterio específico. La hora de inicio de instalación es definida por la programación de la tarea. Si la configuración **Ejecutar tareas no realizadas** se habilita en las propiedades de la tarea, la tarea se puede ejecutar inmediatamente después de que los dispositivos de destino se activen, o cuando se muevan al grupo de administración de destino.

La instalación forzada consiste en el envío de paquetes de instalación a dispositivos de destino, la copia subsecuente de archivos al recurso admin$ en cada uno de los dispositivos de destino y el registro remoto de los servicios de compatibilidad en esos dispositivos. La entrega de paquetes de instalación a dispositivos de destino se realiza mediante una función de Kaspersky Security Center que garantiza la interacción de la red. Las condiciones siguientes se deben cumplir en este caso:

- Se puede acceder a los dispositivos de destino desde el Servidor de administración o desde el punto de distribución.
- La resolución del nombre para los dispositivos de destino funciona correctamente en la red.
- Los usos compartidos administrativos (admin$) permanecen activados en los dispositivos de destino.
- Los siguientes servicios del sistema están en ejecución en los dispositivos de destino:
  - Servidor (LanmanServer)

    De manera predeterminada, este servicio está en ejecución.
  - Iniciador de procesos de servidor DCOM (DcomLaunch)
  - Asignador de endpoints RPC (RpcEptMapper)
  - Llamada a procedimiento remoto (RpcSs)
- El puerto TCP 445 está abierto en los dispositivos de destino para permitir el acceso remoto a través del Instrumental de administración de Windows.

  TCP 139, UDP 137 y UDP 138 se usan en protocolos más antiguos y ya no son necesarios para las aplicaciones actuales.

  En el firewall, se deben permitir puertos de acceso saliente dinámicos para las conexiones desde el Servidor de administración y los puntos de distribución a los dispositivos de destino.
- Se permiten configuraciones de seguridad de la política de dominio de Active Directory para el funcionamiento del protocolo NTLM durante el despliegue del Agente de red.
- En los dispositivos de destino que ejecutan Microsoft Windows XP, el modo de uso compartido simple de archivos está deshabilitado.
- En los dispositivos de destino, el modelo de seguridad y uso compartido de acceso se configura como *Clásico: los usuarios locales se autentican como ellos mismos*. De ninguna manera puede ser *Invitado únicamente: los usuarios locales se autentican como invitados*.
- Los dispositivos de destino son miembros del dominio, o bien se crean cuentas uniformes con derechos de administrador en los dispositivos de destino de antemano.

Para desplegar correctamente el Agente de red u otras aplicaciones en un dispositivo que no está unido a un dominio de Active Directory de Windows Server 2003 o posterior, debe deshabilitar el Control de cuentas de usuario (UAC) remoto en el dispositivo. UAC remoto es una de las razones que impide que las cuentas de administradores locales accedan a admin$, lo que es necesario para el despliegue forzado del Agente de red u otras aplicaciones. Si deshabilita UAC remoto, no interfiere con UAC local.

Durante la instalación en dispositivos nuevos que todavía no se han asignado a ninguno de los grupos de administración de Kaspersky Security Center, puede abrir las propiedades de la tarea de instalación remota y especificar el grupo de administración al cual los dispositivos se moverán después de la instalación del Agente de red.

Al crear una tarea de grupo, tenga en cuenta que cada tarea de grupo afecta a todos los dispositivos en todos los grupos anidados dentro de un grupo seleccionado. Por lo tanto, debe evitar duplicar las tareas de instalación en los subgrupos.

Una forma simplificada de crear tareas para la instalación forzada de aplicaciones es la instalación automática. Para hacerlo, abra las propiedades del grupo de administración, abra la lista de paquetes de instalación y seleccione los que se deben instalar en dispositivos de este grupo. Como resultado, los paquetes de instalación seleccionados se instalarán automáticamente en todos los dispositivos de este grupo y todos sus subgrupos. El intervalo de tiempo durante el cual los paquetes se instalarán depende del rendimiento de la red y el número total de dispositivos conectados a una red.

Para reducir la carga en el Servidor de administración durante la entrega de paquetes de instalación a dispositivos de destino, puede seleccionar la instalación a través de puntos de distribución en la tarea de instalación. Tenga en cuenta que este método de instalación aplica una carga significativa a dispositivos que actúan como puntos de distribución. Por lo tanto, se recomienda seleccionar dispositivos que cumplan con los requisitos de los puntos de distribución. Si usa puntos de distribución, debe asegurarse de que estén presentes en cada una de las subredes aisladas que alojan los dispositivos de destino.

El uso de puntos de distribución como centros de instalación locales también puede ser útil al realizar la instalación en dispositivos en subredes comunicadas con el Servidor de administración mediante un canal de capacidad reducida, mientras que un canal más amplio está disponible entre dispositivos en la misma subred.

El espacio libre del disco en la partición con la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit debe superar, en gran cantidad, el tamaño total de los paquetes de distribución de aplicaciones instaladas.

## Ejecución de paquetes independientes creados por Kaspersky Security Center

Los métodos anteriormente descritos para el despliegue inicial del Agente de red y de otras aplicaciones no siempre se pueden implementar porque no es posible cumplir con todas las condiciones aplicables. En tales casos, puede crear un archivo ejecutable común llamado un *paquete de instalación independiente* a través de Kaspersky Security Center, usando paquetes de instalación con la configuración de instalación relevante preparada por el administrador. El paquete de instalación independiente se almacena en la carpeta compartida de Kaspersky Security Center.

Puede usar Kaspersky Security Center para enviar a usuarios seleccionados un mensaje de correo electrónico que contenga un vínculo a este archivo en la carpeta compartida, e indicarles que ejecuten el archivo (en el modo interactivo, o con la clave "-s" para la instalación silenciosa). Puede adjuntar el paquete de instalación independiente a un mensaje de correo electrónico y luego enviarlo a los usuarios de dispositivos que no tienen acceso a la carpeta compartida de Kaspersky Security Center. El administrador también puede copiar el paquete independiente a una unidad extraíble, entregarlo a un dispositivo relevante, y luego ejecutarlo más adelante.

Puede crear un paquete independiente desde un paquete del Agente de red, un paquete de otra aplicación (por ejemplo, la aplicación de seguridad), o ambos. Si el paquete independiente se ha creado desde el Agente de red y otra aplicación, la instalación se inicia con el Agente de red.

Al crear un paquete independiente con el Agente de red, puede especificar el grupo de administración en el cual los dispositivos nuevos (esos que no se han asignado a ninguno de los grupos de administración) automáticamente se moverá cuando la instalación del Agente de red se complete en ellos.

Los paquetes independientes se pueden ejecutar en el modo interactivo (de forma predeterminada), mostrando el resultado para la instalación de aplicaciones que contienen, o se pueden ejecutar en el modo silencioso (cuando se ejecutan con la clave "-s"). El modo silencioso se puede utilizar para la instalación desde scripts (por ejemplo, desde scripts configurados para ejecutarse tras la instalación de una imagen de sistema operativo). El resultado de instalación en el modo silencioso está determinado por el código de devolución del proceso.

El Agente de red independiente para Linux tiene una dependencia opcional de la utilidad nmap. Si falta la utilidad nmap o es anterior a la versión 6.0, no se admite la funcionalidad Broadcast DHCP Discover.

## Opciones para la instalación manual de aplicaciones

Los administradores o los usuarios experimentados pueden instalar las aplicaciones manualmente en el modo interactivo. Pueden usar los paquetes de distribución originales o paquetes de instalación generados por ellos y almacenados en la carpeta compartida de Kaspersky Security Center. De forma predeterminada, los instaladores se ejecutan en modo interactivo y les indican a los usuarios todos los valores requeridos. Sin embargo, al ejecutar el proceso setup.exe desde el origen de un paquete de instalación con la clave "-s", el instalador se ejecutará en el modo silencioso y con la configuración que se ha definido al configurar el paquete de instalación.

> Al ejecutarse setup.exe desde el origen de un paquete de instalación almacenado en la carpeta compartida de Kaspersky Security Center, el paquete se copiará primero a una carpeta local temporal, y luego el instalador de la aplicación se ejecutará desde la carpeta local.

## Crear un archivo MST

Para transformar el contenido de un paquete MSI y aplicar la configuración personalizada a un archivo MSI existente, debe crear un archivo de transformación en formato MST. Para hacerlo debe usar el editor Orca.exe, que se incluye en el SDK de Windows.

*Para crear un archivo MST:*

1. Ejecute el editor Orca.exe.
2. Vaya a la pestaña **Archivo** y, en el menú, haga clic en **Abrir**.
3. Seleccione el archivo Kaspersky Network Agent.msi.
4. Vaya a la pestaña **Transformación** y, en el menú, seleccione **Nueva transformación**.
5. En la columna **Tablas**, seleccione **Propiedad** y escriba los siguientes valores:
   - *EULA=1*
   - *SERVERADDRESS=<dirección del Servidor de administración>*

   Haga clic en el botón **Guardar**.
6. Vaya a la pestaña **Transformar** y, en el menú, seleccione **Generar transformación**.
7. En la ventana que se abre, especifique el nombre del archivo de transformación a crear y, luego, haga clic en el botón **Guardar**.

Se guarda el archivo MST.

# Instalación remota de aplicaciones en dispositivos en los que se encuentra instalado el Agente de red

Si un Agente de red operable conectado al Servidor de administración principal (o a alguno de sus Servidores secundarios) está conectado en un dispositivo, puede actualizar el Agente de red en este dispositivo, así como instalar, actualizar o eliminar cualquier aplicación admitida a través del Agente de red.

Puede habilitar esta opción al seleccionar la opción **Con el Agente de red** en las propiedades de la tarea de instalación remota.

Si esta opción se selecciona, los paquetes de instalación con la configuración de instalación definida por el administrador se transferirán a los dispositivos de destino a través de canales de comunicación entre l Agente de red y el Servidor de administración.

Para optimizar la carga del Servidor de administración y minimizar el tráfico entre el Servidor de administración y los dispositivos, es útil asignar puntos de distribución en cada red remota o en cada dominio de transmisión (consulte las secciones "Acerca de los puntos de distribución" y "Creación de una estructura de grupos de administración y asignación de puntos de distribución"). En este caso, los paquetes de instalación y la configuración del instalador se distribuyen desde el Servidor de administración hacia los dispositivos de destino a través de puntos de distribución.

Además, puede usar puntos de distribución para la transmisión (multidifusión) y la distribución de paquetes de instalación, lo que permite reducir el tráfico de red considerablemente a la hora de instalar aplicaciones en forma remota.

Al transferir paquetes de instalación a los dispositivos de destino a través de canales de comunicación entre los Agentes de red y el Servidor de administración, todos los paquetes de instalación que se han preparado para la transferencia también se almacenarán en cache en la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. Al usar múltiples paquetes de instalación de gran tamaño y de diversos tipos e involucrar a un gran número de puntos de distribución, el tamaño de esta carpeta puede aumentar significativamente.

Los archivos no se pueden eliminar desde la carpeta FTServer manualmente. Cuando los paquetes de instalación originales se eliminen, los datos correspondientes automáticamente se eliminarán de la carpeta FTServer.

Los datos recibidos por los puntos de distribución se guardan en la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp.

Los archivos no se pueden eliminar de la carpeta $FTCITmp manualmente. Como las tareas usan los datos de esta carpeta completa, los contenidos de esta carpeta se eliminarán automáticamente.

Como los paquetes de instalación se distribuyen por canales de comunicación entre el Servidor de administración y los Agentes de red desde un repositorio intermedio en un formato optimizado para transferencias de red, ningún cambio se permite en paquetes de instalación almacenados en la carpeta original de cada paquete de instalación. Esos cambios no serán automáticamente registrados por el Servidor de administración. Si tiene que modificar los archivos de los paquetes de instalación manualmente (aunque se recomiendan evitar esta situación), debe modificar cualquiera de las configuraciones de un paquete de instalación en la Consola de administración. La modificación de la configuración de un paquete de instalación en la Consola de administración hace que el Servidor de administración actualice la imagen del paquete en el caché que se ha preparado para la transferencia hacia los dispositivos de destino.

## Opciones para controlar el reinicio de los dispositivos en la tarea de instalación remota

Los dispositivos a menudo necesitan un reinicio para completar la instalación remota de aplicaciones (en particular en Windows).

Si usa la tarea de instalación remota de Kaspersky Security Center, en el Asistente para crear nueva tarea o en la ventana de propiedades de la tarea que se ha creado (sección **Reinicio del sistema operativo**), puede seleccionar la acción para realizar cuando el dispositivo de Windows requiera un reinicio:

- **No reiniciar el dispositivo**. En este caso, ningún reinicio automático se realizará. Para completar la instalación, debe reiniciar el dispositivo (por ejemplo, manualmente o a través de la tarea de administración del dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para tareas de instalación en servidores y otros dispositivos donde la operación continua sea crítica.

- **Reiniciar el dispositivo**. En este caso, el dispositivo siempre se reinicia automáticamente si se requiere un reinicio para la finalización de la instalación. Esta opción es útil para tareas de instalación en dispositivos que proporcionan pausas habituales en su operación (cierre o reinicio).

- **Solicitar al usuario una acción**. En este caso, el recordatorio de reinicio se muestra en la pantalla del dispositivo cliente, que le solicita al usuario que lo reinicie manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). La opción **Solicitar al usuario una acción** es la más conveniente para las estaciones de trabajo donde los usuarios necesitan la posibilidad de seleccionar el horario más cómodo para un reinicio.

## Conveniencia de actualizar las bases de datos en el paquete de instalación de una aplicación de seguridad

Antes de comenzar con el despliegue de la protección, debe tener en cuenta la posibilidad de actualizar las bases de datos antivirus (incluidos los módulos de los parches automáticos), que se envían junto con el paquete de distribución de la aplicación de seguridad. Es útil actualizar las bases de datos en el paquete de instalación de la aplicación antes de dar inicio al despliegue (por ejemplo, usando el comando correspondiente en el menú contextual de un paquete de instalación seleccionado). Con ello se reducirá el número de reinicios necesarios para completar el despliegue de la protección en los dispositivos de destino.

## Utilización de herramientas para la instalación remota de aplicaciones en Kaspersky Security Center para ejecutar archivos ejecutables relevantes en dispositivos administrados

Mediante el Asistente de nuevo paquete, puede seleccionar cualquier archivo ejecutable y definir la configuración de la línea de comandos para ello. Para esto, puede agregar al paquete de instalación el archivo seleccionado o la carpeta completa en la cual este archivo se almacena. A continuación, debe crear la tarea de instalación remota y seleccionar el paquete de instalación que se ha creado.

Mientras la tarea se está ejecutando, el archivo ejecutable especificado con la configuración definida del comando solicitado se ejecutará en dispositivos de destino.

Si usa instaladores en el formato de Microsoft Windows Installer (MSI), Kaspersky Security Center analiza los resultados de instalación por medio de herramientas estándares.

Si una licencia de Administración de vulnerabilidades y parches está disponible, Kaspersky Security Center (al crear un paquete de instalación para cualquier aplicación admitida en el entorno corporativo) también usa reglas para la instalación y el análisis de resultados de instalación que están en su base de datos actualizable.

De otra forma, la tarea predeterminada para archivos ejecutables espera la finalización del proceso en ejecución, y de todos sus procesos secundarios. Después de la finalización de todos los procesos en ejecución, la tarea se completará correctamente sin tener en cuenta el código de devolución del proceso inicial. Para cambiar el comportamiento de esta tarea, antes de crear la tarea, tiene que modificar manualmente los archivos .kpd que fueron generados por Kaspersky Security Center en la carpeta del paquete de instalación recién creado y sus subcarpetas.

Los archivos .kpd utilizan la codificación ASCII. Los archivos .kud utilizan la codificación Unicode.

Para que la tarea no espere la finalización del proceso en ejecución, configure el valor de la configuración Wait en 0 en la sección [SetupProcessResult]:

```
[SetupProcessResult]
Wait=0
```

Para que la tarea espere solo la finalización del proceso en ejecución en Windows, no la finalización de todos los procesos secundarios, configure el valor de la configuración WaitJob en 0 en la sección [SetupProcessResult], por ejemplo:

```
[SetupProcessResult]
WaitJob=0
```

Para que la tarea se complete con éxito o devuelva un error según el código de retorno del proceso en ejecución, cree un archivo .bat ejecutable que guarde el código de error en un archivo, por ejemplo:

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

Y luego modifique los archivos .kud que generó Kaspersky Security Center en la carpeta del paquete de instalación recién creado:

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0=La instalación finalizó correctamente
[SetupMainResult_ErrorCodes]
1=Installation script error
2=Custom error
```

En este caso, cualquier código diferente de los enumerados causará la devolución de un error.

Para mostrar una cadena con un comentario sobre la finalización correcta de la tarea o un error en los resultados de la tarea, escriba breves descripciones de errores correspondientes a códigos de devolución del proceso en las secciones [SetupProcessResult_SuccessCodes] y [SetupProcessResult_ErrorCodes], por ejemplo:

```
[SetupProcessResult_SuccessCodes]
0= La instalación finalizó correctamente
3010=Se debe reiniciar el dispositivo para completar la instalación
[SetupProcessResult_ErrorCodes]
1602=instalación cancelada por el usuario
1603=Error importante durante la instalación
```

Para usar las herramientas de Kaspersky Security Center para administrar el reinicio del dispositivo (si se requiere un reinicio para completar una operación), enumere los códigos de devolución del proceso que indican que un reinicio se debe realizar, en la sección [SetupProcessResult_NeedReboot]:

```
[SetupProcessResult_NeedReboot]
3010=
```

## Supervisión del despliegue

Para supervisar el despliegue de Kaspersky Security Center y asegurarse de que una aplicación de seguridad y el Agente de red se instalen en los dispositivos administrados, tiene que comprobar el semáforo en la sección **Despliegue**. Este semáforo se localiza en el espacio de trabajo del nodo del Servidor de administración en la ventana principal de la Consola de administración. El semáforo refleja el estado del despliegue. El número de dispositivos con el Agente de red y aplicaciones de seguridad instalados se muestra al lado del semáforo. Cuando cualquier tarea de instalación se está ejecutando, puede supervisar su progreso aquí. Si se presentan errores de instalación, el número de errores se muestra aquí. Puede ver los detalles de cualquier error haciendo clic en el enlace.

También puede usar el gráfico de despliegue en el espacio de trabajo de la carpeta **Dispositivos administrados** en la pestaña **Grupos**. El gráfico refleja el proceso de despliegue, ya que muestra el número de dispositivos sin Agente de red, con Agente de red, o con Agente de red y una aplicación de seguridad.

Para obtener más información sobre el progreso del despliegue (o la operación de una tarea de instalación específica), abra la ventana de resultados de la tarea de instalación remota relevante: Haga clic en la tarea con el botón derecho del ratón y seleccione **Resultados** el menú contextual. La ventana muestra dos listas: la superior contiene los estados de las tareas en dispositivos, mientras que la inferior contiene eventos de tareas en el dispositivo que está seleccionado actualmente en la lista superior.

La información sobre los errores de despliegue se agrega al registro de eventos de Kaspersky en el Servidor de administración. La información sobre errores también está disponible a través de la selección de eventos correspondiente en el nodo del Servidor de administración en la pestaña **Eventos**.

## Configuración de instaladores

Esta sección proporciona la información sobre los archivos de instaladores de Kaspersky Security Center y la configuración de instalación, así como recomendaciones sobre cómo instalar el Servidor de administración y el Agente de red en el modo silencioso.

## Información general

Los Instaladores de los componentes de Kaspersky Security Center 15.1 (Servidor de administración, Agente de red y Consola de administración) se basan en la tecnología de Windows Installer. Un paquete MSI es el núcleo de un instalador. Este formato de paquetes permite usar todas las ventajas proporcionadas por Windows Installer: escalabilidad, disponibilidad de un sistema de parches, sistema de transformación, instalación centralizada a través de soluciones de terceros y registro transparente con el sistema operativo.

## Instalación en modo silencioso (con un archivo de respuesta)

Los instaladores de Servidor de administración y el Agente de red tienen la función de trabajar con el archivo de respuesta (ss_install.xml), donde los parámetros para la instalación en el modo silencioso sin la participación del usuario se integran. El archivo ss_install.xml se localiza en la misma carpeta que el paquete MSI; se utiliza automáticamente durante la instalación en el modo silencioso. Puede habilitar el modo de instalación silenciosa con el modificador de línea de comandos "/s".

Una descripción general de un ejemplo de ejecución se presenta a continuación:

```
setup.exe /s
```

Antes de iniciar el instalador en modo silencioso, lea el Contrato de licencia de usuario final (también denominado EULA, por las siglas del término en inglés). Si el kit de distribución de Kaspersky Security Center no incluye un archivo TXT con el texto del EULA, puede descargar el archivo desde el sitio web de Kaspersky.

El archivo ss_install.xml es una instancia del formato interno de los parámetros del instalador de Kaspersky Security Center. Los paquetes de distribución contienen el archivo ss_install.xml con los parámetros predeterminados.

No modifique el archivo ss_install.xml manualmente. Este archivo puede modificarse mediante las herramientas de Kaspersky Security Center al modificar los parámetros de los paquetes de instalación en la Consola de administración.

*Para modificar el archivo de respuesta para la instalación del Servidor de administración:*

1. Abra el paquete de distribución de Kaspersky Security Center. Si utiliza un archivo EXE de paquete completo, descomprímalo.

2. Desde la carpeta Server, abra la línea de comandos y ejecute el siguiente comando:
   ```
   setup.exe /r ss_install.xml
   ```
   Se ejecuta el instalador de Kaspersky Security Center.

3. Siga los pasos del asistente para configurar la instalación de Kaspersky Security Center.

   Cuando complete el asistente, el archivo de respuesta se modifica automáticamente de acuerdo con la nueva configuración que especificó.

## Instalación del Agente de red en modo silencioso (sin un archivo de respuesta)

Puede instalar el Agente de red con un paquete msi solo, especificando los valores de las propiedades MSI del modo estándar. Esta situación permite que el Agente de red se instale usando directivas de grupo.

No cambie el nombre del paquete de instalación Kaspersky Network Agent.msi. De lo contrario, pueden aparecer errores de instalación cuando actualice el Agente de red más adelante.

Para evitar conflictos entre los parámetros definidos mediante las propiedades MSI y los parámetros definidos en el archivo de respuesta, puede desactivar el archivo de respuesta al configurar la propiedad `DONT_USE_ANSWER_FILE=1`. El archivo MSI se encuentra en el paquete de distribución de Kaspersky Security Center, en la carpeta Packages\NetAgent\exec. Un ejemplo de una ejecución del instalador del Agente de red con un paquete msi es de la forma siguiente.

La instalación del Agente de red en modo no interactivo requiere la aceptación de los términos del Contrato de licencia de usuario final. Utilice el parámetro de `EULA=1` solo si ha leído, entendido y aceptado completamente los términos del Contrato de licencia de usuario final.

Ejemplo:

```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

También puede definir los parámetros de instalación para un paquete msi al preparar el archivo de respuesta de antemano (uno con la extensión mst). Este comando aparece de la forma siguiente:

Ejemplo:

```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

Puede especificar varios archivos de respuesta en un mismo comando.

Si desea actualizar el Agente de red con Windows Installer, ejecute el siguiente comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

## Configuración de instalación parcial a través de setup.exe

Al ejecutar la instalación de aplicaciones a través de setup.exe, puede agregar los valores de cualquier propiedad de MSI al paquete MSI.

Este comando aparece de la forma siguiente:

Ejemplo:

```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

## Parámetros de instalación del Servidor de administración

En la siguiente tabla, se describen las propiedades MSI que puede configurar al instalar el Servidor de administración. Todos los parámetros son opcionales, excepto EULA y PRIVACYPOLICY.

| Propiedad MSI | Descripción | Valores disponibles |
|---|---|---|
| EULA | Aceptación de los términos del Contrato de licencia (requerido). | • 1: he leído, comprendo y acepto en su totalidad los términos del Contrato de licencia de usuario final.<br>• Otro valor o ningún valor: no acepto los términos del Contrato de licencia (no se realizará la instalación). |
| PRIVACYPOLICY | Aceptación de los términos de la Política de privacidad (obligatorio) | • 1: entiendo y acepto que mis datos serán tratados y transmitidos (incluso a otros países) según lo descrito en la Política de privacidad. Confirmo que he leído y que comprendo en su totalidad la Política de privacidad.<br>• Otro valor o ningún valor: no acepto los términos de la Política de privacidad (no se realizará la instalación). |
| INSTALLATIONMODETYPE | Tipo de instalación del Servidor de administración | • Standard.<br>• Custom. |
| INSTALLDIR | Carpeta de instalación de la aplicación | Valor de cadena. |
| ADDLOCAL | Lista de componentes para instalar (separados por comas) | CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86.<br>Lista mínima de componentes que se requieren para instalar el Servidor de administración:<br>`ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86` |
| NETRANGETYPE | Tamaño de la red | • NRT_1_100: de 1 a 100 dispositivos.<br>• NRT_100_1000: de 101 a 1000 dispositivos.<br>• NRT_GREATER_1000: más de 1 000 dispositivos. |
| SRV_ACCOUNT_TYPE | Modo de especificar el usuario con el que funcionará el servicio del Servidor de administración | • SrvAccountDefault: la cuenta de usuario se creará automáticamente.<br>• SrvAccountUser: la cuenta de usuario se define manualmente. |
| SERVERACCOUNTNAME | Nombre de usuario para el servicio | Valor de cadena. |
| SERVERACCOUNTPWD | Contraseña del usuario para el servicio | Valor de cadena. |
| DBTYPE | Tipo de base de datos | • MySQL: se utilizará una base de datos MySQL o MariaDB.<br>• MSSQL: se usará la base de datos de Microsoft SQL Server (SQL Express). |
| MYSQLSERVERNAME | Nombre completo del servidor MySQL o MariaDB | Valor de cadena. |
| MYSQLSERVERPORT | Número de puerto para la conexión al servidor MySQL o MariaDB | Valor numérico. |
| MYSQLDBNAME | Nombre de la base de datos del servidor MySQL o MariaDB | Valor de cadena. |
| MYSQLACCOUNTNAME | Nombre de usuario para la conexión con la base de datos del servidor MySQL o MariaDB | Valor de cadena. |
| MYSQLACCOUNTPWD | Contraseña de usuario para la conexión con la base de datos del servidor MySQL o MariaDB | Valor de cadena. |
| MSSQLCONNECTIONTYPE | Tipo de uso de la base de datos MSSQL | • InstallMSSEE: instalar desde un paquete.<br>• ChooseExisting: usar un servidor instalado. |
| MSSQLSERVERNAME | Nombre completo de la instancia de SQL Server | Valor de cadena. |

| Propiedad MSI | Descripción | Valores disponibles |
|---|---|---|
| MSSQLDBNAME | Nombre de la base de datos de SQL Server | Valor de cadena. |
| MSSQLAUTHTYPE | Método de autenticación para conectarse a SQL Server | • Windows.<br>• SQLServer. |
| MSSQLACCOUNTNAME | Nombre de usuario para conectarse a SQL Server en modo SQLServer | Valor de cadena. |
| MSSQLACCOUNTPWD | Contraseña del usuario para conectarse a SQL Server en modo SQLServer | Valor de cadena. |
| CREATE_SHARE_TYPE | Forma de especificar la carpeta compartida | • Create: Crear una carpeta compartida nueva. En este caso, las propiedades siguientes se deben definir:<br>  • SHARELOCALPATH: ruta a una carpeta local.<br>  • SHAREFOLDERNAME: nombre de red de una carpeta.<br>• Nulo: se debe especificar la propiedad EXISTSHAREFOLDERNAME. |
| EXISTSHAREFOLDERNAME | Ruta completa a una carpeta compartida existente | Valor de cadena. |
| SERVERPORT | Número de puerto para conectarse al Servidor de administración | Valor numérico. |
| SERVERSSLPORT | Número de puerto para conectarse al Servidor de administración con SSL | Valor numérico. |
| SERVERADDRESS | Dirección del Servidor de administración | Valor de cadena. |
| SERVERCERT2048BITS | Tamaño de la clave para el certificado del Servidor de administración (bits) | • 1: El tamaño de la clave para el certificado del Servidor de administración es de 2048 bits.<br>• 0: el tamaño de la clave para el certificado del Servidor de administración es de 1024 bits.<br>• Si no se especifica ningún valor, el tamaño de la clave para el certificado del Servidor de administración es 2048 bits. |
| MOBILESERVERADDRESS | Dirección del Servidor de administración para la conexión de dispositivos móviles; esta propiedad se ignorará si no se ha seleccionado el componente MobileSupport | Valor de cadena. |

## Agente de red: parámetros de instalación

La tabla a continuación describe las propiedades MSI que puede configurar al instalar el Agente de red. Todos los parámetros son opcionales, excepto EULA y SERVERADDRESS.

Parámetros de instalación del Agente de red en modo no interactivo

| Propiedad MSI | Descripción | Valores disponibles |
|---|---|---|
| EULA | Aceptación de los términos del Contrato de licencia | • 1: Confirmo que he leído completamente, entiendo y acepto los términos y las condiciones de este Contrato de licencia de usuario final.<br>• 0: No acepto los términos del Contrato de licencia (no se realiza la instalación).<br>• Sin valor: no acepto los términos del Contrato de licencia (no se realiza la instalación). |
| DONT_USE_ANSWER_FILE | Lea la configuración de instalación desde el archivo de respuesta | • 1—No usar.<br>• Otro valor o ningún valor—Leer. |

| Propiedad MSI | Descripción | Valores disponibles |
|---|---|---|
| INSTALLDIR | Ruta a la carpeta de instalación del Agente de red | Valor de cadena. |
| SERVERADDRESS | Dirección del Servidor de administración (obligatoria) | Valor de cadena. |
| SERVERPORT | Número de un puerto para la conexión al Servidor de administración | Valor numérico. |
| SERVERSSLPORT | Número del puerto para conexión cifrada al Servidor de administración usando el protocolo SSL | Valor numérico. |
| USESSL | Usar una conexión SSL o no | • 1: Usar<br>• Otro valor o ningún valor: No usar |
| OPENUDPPORT | Abrir un puerto UDP o no | • 1: Abrir<br>• Otro valor o ningún valor: No abrir |
| UDPPORT | Número de puerto UDP | Valor numérico. |
| USEPROXY | Usar un servidor proxy o no.<br>Por motivos de compatibilidad, no se recomienda especificar la configuración de la conexión del proxy en la configuración del paquete de instalación del Agente de red. | • 1: Usar<br>• Otro valor o ningún valor: No usar |
| PROXYLOCATION (PROXYADDRESS:PROXYPORT) | Dirección del proxy y número de puerto para la conexión con el servidor proxy | Valor de cadena. |
| PROXYLOGIN | Cuenta para la conexión con un servidor proxy | Valor de cadena. |
| PROXYPASSWORD | Contraseña de la cuenta para conectarse al servidor proxy (No indique ningún detalle de las cuentas con privilegios en los parámetros de los paquetes de instalación). | Valor de cadena. |
| GATEWAYMODE | Modo de uso de la puerta de enlace de conexión | • 0: No usar la puerta de enlace de conexión<br>• 1: Use este Agente de red como puerta de enlace de conexión<br>• 2: Conectarse al Servidor de administración mediante una puerta de enlace de conexión |
| GATEWAYADDRESS | Dirección de la puerta de enlace de conexión | Valor de cadena. |
| CERTSELECTION | Método de recibir un certificado | • GetOnFirstConnection; Reciba un certificado del Servidor de administración<br>• GetExistent: Seleccionar un certificado existente. Si se selecciona esta opción, se deberá especificar la propiedad CERTFILE |
| CERTFILE | Ruta al archivo de certificado | Valor de cadena. |
| VMVDI | Habilitar el modo dinámico para la Infraestructura de escritorio virtual (VDI) | • 1: Habilitar.<br>• 0: No habilitar.<br>• Sin valor: No habilitar. |
| VMOPTIMIZE | Determina si el Agente de red usará los ajustes de configuración optimizados para hipervisores | • 1: Habilitar.<br>• 0: No habilitar.<br>• Sin valor: No habilitar. |

| Propiedad MSI | Descripción | Valores disponibles |
| --- | --- | --- |
| LAUNCHPROGRAM | Ejecutar el inicio del servicio del Agente de red después de la instalación. El parámetro se ignora si VMVDI=1 | • 1: Iniciar<br>• Otro valor o ningún valor: No iniciar |
| NAGENTTAGS | Etiqueta para el Agente de red (tiene prioridad sobre la etiqueta dada en el archivo de respuestas) | Valor de cadena. |

# Infraestructura virtual

Kaspersky Security Center admite el uso de máquinas virtuales. Puede instalar el Agente de red y una aplicación de seguridad en cada máquina virtual; también puede proteger todas las máquinas virtuales a nivel hipervisor. En el primer caso, las máquinas pueden protegerse con cualquier aplicación de seguridad estándar o con Kaspersky Security for Virtualization Light Agent. En el segundo caso, puede usar Kaspersky Security for Virtualization Agentless.

Kaspersky Security Center está preparado para operar con máquinas virtuales que puedan revertir su estado a un punto anterior.

## Sugerencias sobre la reducción de la carga en máquinas virtuales

Al instalar el Agente de red en una máquina virtual, le aconsejan que considere la deshabilitación de algunas funciones de Kaspersky Security Center que parecen ser de poco uso para máquinas virtuales.

Al instalar el Agente de red en una máquina virtual o en una plantilla querida para la generación de máquinas virtuales, recomendamos realizar las siguientes acciones:

- Si está ejecutando una instalación remota, en la ventana de propiedades del paquete de instalación del Agente de red, en la sección **Avanzado**, seleccione la opción **Optimizar la configuración para VDI**.
- Si está ejecutando una instalación interactiva a través de un Asistente, en la ventana Asistente, seleccione la opción **Optimizar la configuración del Agente de red para la infraestructura virtual**.

Seleccionar esas opciones cambia la configuración del Agente de red de modo que las funciones siguientes permanezcan desactivadas de forma predeterminada (antes de aplicar una directiva):

- Recopilación de información acerca del software instalado
- Recopilación de información acerca del hardware
- Recopilación de información acerca de las vulnerabilidades detectadas
- Recopilación de información acerca de las actualizaciones necesarias

Por lo general, esas funciones no son necesarias en máquinas virtuales porque usan el software uniforme y el hardware virtual.

La deshabilitación de las funciones es irreversible. Si alguna de las funciones desactivadas se requiere, la puede habilitar a través de la directiva del Agente de red, o a través de la configuración local del Agente de red. La configuración local del Agente de red está disponible a través del menú contextual del dispositivo relevante en la Consola de administración.

## Compatibilidad con máquinas virtuales dinámicas

Kaspersky Security Center es compatible con las máquinas virtuales dinámicas. Si existe una infraestructura virtual en la red de la organización, las máquinas virtuales dinámicas (temporales) se pueden utilizar en ciertos casos. Las máquinas virtuales dinámicas se crean con nombres únicos según una plantilla que preparada por el administrador. El usuario trabaja en la máquina virtual un tiempo, luego, después de apagarse, esta máquina virtual se eliminará de la infraestructura virtual. Si se ha desplegado Kaspersky Security Center en la red de la organización, se agregará una máquina virtual con el Agente de red instalado a la base de datos del Servidor de administración. Después de que desactive una máquina virtual, la entrada correspondiente también se debe eliminar de la base de datos de Servidor de administración.

Para hacer funcional la función de eliminación automática de entradas en máquinas virtuales, al instalar un Agente de red en una plantilla para máquinas virtuales dinámicas, seleccione la opción **Habilitar modo dinámico para VDI**:

- Para la instalación remota: En la ventana de propiedades del paquete de instalación del Agente de red (Sección **Avanzado**)
- Para la instalación interactiva: en el Asistente de instalación del Agente de red

> Evite seleccionar la opción **Habilitar modo dinámico para VDI** al instalar el Agente de red en dispositivos físicos.

Si desea que los eventos de las máquinas virtuales dinámicas se almacenen en el Servidor de administración durante un tiempo después de eliminar esas máquinas virtuales, en la ventana de propiedades del Servidor de administración, en la sección **Repositorio de eventos**, marque la opción **Almacenar los eventos de los dispositivos eliminados** y especifique el plazo de almacenamiento máximo para los eventos (en días).

> No recomendamos habilitar el cifrado de unidades en máquinas virtuales dinámicas.

## Soporte de copia de máquinas virtuales

Copiar una máquina virtual que tiene el Agente de red instalado y crear una máquina virtual a partir de una plantilla que tiene el Agente de red instalado son procedimientos idénticos al de capturar y copiar una imagen de disco duro como método para desplegar el Agente de red. Por ello, en general, si copia una máquina virtual, deberá realizar las mismas acciones que si hubiera copiado una imagen de disco para desplegar el Agente de red.

Sin embargo, los dos casos que se describen a continuación muestran el Agente de red que detecta la copia automáticamente. Debido a los motivos indicados anteriormente, no tiene que realizar las operaciones sofisticadas descritas en la sección "Despliegue con una imagen de disco duro capturada de un dispositivo":

- La opción **Habilitar modo dinámico para VDI** se seleccionó cuando el Agente de red se instaló: después de cada reinicio del sistema operativo, esta máquina virtual se reconocerá como un dispositivo nuevo, sin tener en cuenta si se ha copiado.

- Uno de los siguientes hipervisores está en uso: VMware™, HyperV® o Xen®: Agente de red detecta la copia de la máquina virtual mediante los id. modificados del hardware virtual.

El análisis de cambios en el hardware virtual no es absolutamente fiable. Antes de aplicar este método extensamente, lo debe probar en un pequeño grupo de máquinas virtuales para la versión del hipervisor actualmente usado en su organización.

## Soporte de reversión del sistema de archivos para dispositivos con Agente de red

Kaspersky Security Center es una aplicación distribuida. El revertir el sistema de archivos a un estado anterior en un dispositivo con Agente de red instalado llevará a la desincronización de datos y funcionamiento incorrecto de Kaspersky Security Center.

El sistema de archivos (o una parte de él) se puede revertir en los casos siguientes:

- Al copiar una imagen del disco duro.

- Al restaurar un estado de la máquina virtual por medio de la infraestructura virtual.

- Al restaurar datos desde una copia de seguridad o un punto de recuperación.

Las situaciones según las cuales el software de terceros en dispositivos con el Agente de red instalado afecta la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ son solo situaciones críticas para Kaspersky Security Center. Por lo tanto, siempre debe excluir esta carpeta del procedimiento de recuperación, de ser posible.

Como las reglas del lugar de trabajo de algunas organizaciones proporcionan reversiones del sistema de archivos en dispositivos, el soporte de la reversión del sistema de archivos en dispositivos con Agente de red instalado se agregó a Kaspersky Security Center a partir de la versión 10 Maintenance Release 1 (Servidor de administración y Agentes de red deben ser de la versión 10 Maintenance Release 1 o posterior). Cuando se detecta, esos dispositivos automáticamente se conectan de nuevo al Servidor de administración con limpieza de datos completa y sincronización completa.

De forma predeterminada, el soporte de la detección de reversión del sistema de archivos está habilitado en Kaspersky Security Center 15.1.

Siempre que sea posible, evite deshacer la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ en dispositivos con el Agente de red instalado, porque la resincronización completa de datos requiere una gran cantidad de recursos.

Una reversión del estado del sistema no se permite en absoluto en un dispositivo con el Servidor de administración instalado. Tampoco se aplica a la reversión de la base de datos usada por el Servidor de administración.

Puede restaurar un estado del Servidor de administración desde una copia de seguridad solo con la utilidad estándar klbackup.

## Instalación local de aplicaciones

En esta sección, se describe un procedimiento de instalación de aplicaciones que se pueden instalar solo en dispositivos locales.

Para realizar la instalación local de las aplicaciones en un dispositivo cliente especificado, debe tener derechos de administrador en ese dispositivo.

*Para instalar aplicaciones de manera local en un dispositivo cliente específico:*

1. Instale el Agente de red en el dispositivo cliente y configure la conexión entre el dispositivo cliente y el Servidor de administración.

2. Instale las aplicaciones requeridas en el dispositivo, tal como se describe en las guías de estas aplicaciones.

3. Instale un complemento de administración para cada una de las aplicaciones instaladas en la estación de trabajo del administrador.

Kaspersky Security Center también admite la opción de instalación local de las aplicaciones que usan un paquete de instalación independiente. Kaspersky Security Center no admite la instalación de todas las aplicaciones de Kaspersky.

## Instalación local del Agente de red

*Para instalar el Agente de red en un dispositivo de manera local:*

1. En el dispositivo, ejecute el archivo setup.exe desde el paquete de distribución descargado de Internet. Consulte el siguiente tema para obtener más información: Obtener el paquete de instalación del Agente de red desde el kit de distribución de Kaspersky Security Center.

   Se abre una ventana y se le solicita que seleccione las aplicaciones de Kaspersky que desea instalar.

2. En la ventana de selección de aplicación, haga clic en el vínculo **Instalar solo el Agente de red de Kaspersky Security Center** para iniciar el asistente de instalación del Agente de red. Siga las instrucciones del asistente.

   a. Servidor de administración

   **Puerto**

   Especifica el puerto no SSL que utiliza el Servidor de administración para recibir conexiones de los Agentes de red.

   De forma predeterminada, esta opción está establecida en 14 000.

   **Puerto SSL**

   Especifica el puerto SSL que usa el Servidor de administración para recibir conexiones de los Agentes de red.

   De forma predeterminada, esta opción está establecida en 13 000.

   **Usar SSL para conectarse con el Servidor de administración**

   Si se habilita esta opción, la conexión al Servidor de administración se establecerá a través de un puerto seguro utilizando el protocolo SSL.

   Esta opción está activada de forma predeterminada.

   **Permitir que el Agente de red abra un puerto UDP**

   Si esta opción está habilitada, el instalador abre automáticamente el puerto que usa el Servidor de administración para administrar el dispositivo cliente y recibir información sobre él.

   Esta opción está activada de forma predeterminada.

   **Puerto UDP**

   Le permite configurar el puerto que usa el Servidor de administración para administrar el dispositivo cliente y recibir información sobre él.

   De forma predeterminada, esta opción está establecida en 15 000.

   b. Configuración del servidor proxy

**Usar servidor proxy**

Si esta opción está habilitada, puede especificar las credenciales para la autenticación del servidor proxy.

Le recomendamos que utilice las credenciales de una cuenta que solamente tenga los privilegios mínimos necesarios para completar la autenticación ante el servidor proxy.

Esta opción está deshabilitada de forma predeterminada.

**Dirección**

**Puerto**

**Cuenta**

El nombre de usuario de la cuenta con la que se establece la conexión al servidor proxy.

Le recomendamos que utilice las credenciales de una cuenta que solamente tenga los privilegios mínimos necesarios para completar la autenticación ante el servidor proxy.

**Contraseña**

La contraseña de usuario de la cuenta con la que se establece la conexión al servidor proxy.

Le recomendamos que utilice las credenciales de una cuenta que solamente tenga los privilegios mínimos necesarios para completar la autenticación ante el servidor proxy.

c. Puerta de enlace de conexión

**No usar la puerta de enlace de conexión**

**Usar el Agente de red como una puerta de enlace de conexión en la DMZ**

Seleccione esta opción para usar el Agente de red como puerta de enlace de conexión en la zona desmilitarizada (DMZ) para conectarse al Servidor de administración, comunicarse con él y mantener los datos del Agente de red a salvo durante la transmisión de datos.

**Conectarse al Servidor de administración mediante una puerta de enlace de conexión**

Seleccione esta opción y luego especifique qué dispositivo servirá como puerta de enlace de conexión.

d. **Certificado del Servidor de administración**

e. **Etiquetas del Agente**

f. Configuración avanzada

**Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes**

Recomendamos mantener esta opción habilitada. Puede desactivar esta opción para deshabilitar la actualización y la aplicación de parches automáticas para los componentes de Kaspersky Security Center. El administrador puede volver a habilitar la actualización y la aplicación de parches automáticas más adelante mediante una directiva.

Esta opción está deshabilitada de forma predeterminada.

**Habilitar la protección del servicio del Agente de red**

Cuando esta opción está habilitada, una vez que el Agente de red se encuentre instalado en un dispositivo administrado, no se lo podrá eliminar ni reconfigurar a menos que se tengan los privilegios necesarios. El servicio del Agente de red no se podrá detener. Esta opción no tiene efecto en los controladores de dominio.

Habilite esta opción para proteger el Agente de red en estaciones de trabajo operadas con derechos de administrador local.

Esta opción está deshabilitada de forma predeterminada.

**Habilitar modo dinámico para VDI**

Si habilita esta opción, se habilitará un modo dinámico para infraestructuras de escritorios virtuales (VDI) para el Agente de red instalado en una máquina virtual.

Esta opción está deshabilitada de forma predeterminada.

**Optimice la configuración del Agente de red de Kaspersky Security Center para VDI. Deshabilite el análisis de vulnerabilidades y el inventario de aplicaciones y hardware. Puede editar la configuración actual a través de las directivas del Agente de red.**

Si habilita esta opción, se deshabilitarán las siguientes características de la configuración del Agente de red:

- Recopilación de información acerca del software instalado
- Recopilación de información acerca del hardware
- Recopilación de información acerca de las vulnerabilidades detectadas
- Recopilación de información acerca de las actualizaciones necesarias

Esta opción está deshabilitada de forma predeterminada.

g. **Iniciar la aplicación**

Cuando el asistente de instalación se haya completado, el Agente de red estará instalado en el dispositivo.

Las siguientes herramientas estándares de Microsoft Windows permiten ver las propiedades del servicio del Agente de red de Kaspersky Security Center; también puede iniciar, detener y supervisar la actividad del Agente de red: Administración de equipos/Servicios.

## Instalación del Agente de red en modo silencioso

El Agente de red puede instalarse en modo no interactivo; es decir, sin entrada interactiva de los parámetros de instalación. La instalación no interactiva usa un paquete de Windows Installer (MSI) para el Agente de red. El archivo MSI se encuentra en el paquete de distribución de Kaspersky Security Center, en la carpeta Packages\NetAgent\exec.

No cambie el nombre del paquete de instalación Kaspersky Network Agent.msi. De lo contrario, pueden aparecer errores de instalación cuando actualice el Agente de red más adelante.

La instalación del Agente de red desde el paquete MSI solo es posible en modo silencioso, no se admite la instalación interactiva desde el paquete MSI.

*Para instalar el Agente de red en un dispositivo local en modo no interactivo:*

1. Lea el Contrato de licencia de usuario final. Use el comando a continuación únicamente si comprende y acepta los términos del Contrato de licencia de usuario final.

2. Ejecute el comando

   ```
   msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
   ```

   donde `setup_parameters` es una lista de parámetros y sus respectivos valores, separados por un espacio (`PROP1=PROP1VAL PROP2=PROP2VAL`).

   En la lista de parámetros debe incluir `EULA=1`. De lo contrario, el Agente de red no se instalará.

Si está utilizando la configuración de conexión estándar para Kaspersky Security Center y el Agente de red en dispositivos remotos, ejecute el comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` es la clave para escribir registros. El registro se crea durante la instalación del Agente de red y se guarda en C:\windows\temp\nag_inst.log.

Además de nag_inst.log, la aplicación crea el archivo $klssinstlib.log, que contiene el registro de instalación. Este archivo se almacena en la carpeta %windir%\temp o %temp%. Para solucionar problemas, es posible que usted o un especialista del Servicio de soporte técnico de Kaspersky necesiten ambos archivos de registro: nag_inst.log y $klssinstlib.log.

Si necesita especificar adicionalmente el puerto para la conexión al Servidor de administración, ejecute el comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

El parámetro `SERVERPORT` corresponde al número de puerto para la conexión al Servidor de Administración.

Los nombres y posibles valores de los parámetros que se pueden utilizar al instalar el Agente de red en modo no interactivo se enumeran en la sección Parámetros de instalación del Agente de red.

Si desea actualizar el Agente de red con Windows Installer, ejecute el siguiente comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

## Instalación del Agente de red para Linux en modo silencioso (con un archivo de respuestas)

A la hora de instalar el Agente de red en un dispositivo con Linux, puede utilizar lo que se denomina "archivo de respuestas", un archivo de texto con variables y valores que representan opciones de instalación específicas. El archivo de respuestas permite realizar la instalación en modo no interactivo, es decir, sin involucrar al usuario.

*Para instalar el Agente de red para Linux en modo silencioso:*

1. Complete los preparativos de instalación remota en el dispositivo con Linux pertinente. Descargue el paquete de instalación del Agente de red con el sistema de gestión de paquetes que corresponda, y luego utilice el paquete .deb o .rpm del Agente de red para crear el paquete de instalación remota.

2. Si desea instalar el Agente de red en dispositivos con el sistema operativo SUSE Linux Enterprise Server 15, primero, instale el paquete insserv-compat para configurar el Agente de red.

   Si desea instalar el Agente de Red en dispositivos que utilicen el sistema operativo RED OS 7.3.4 o posterior, o MSVSPHERE 9.2 o posterior, instale el paquete libxcrypt-compat para el correcto funcionamiento del Agente de Red.

3. Lea el Contrato de licencia de usuario final. Siga los pasos a continuación únicamente si comprende y acepta los términos del Contrato de licencia de usuario final.

4. Cree el archivo de respuesta (en formato TXT). El archivo debe contener una lista de variables en formato NOMBRE_DE_LA_VARIABLE=valor_de_la_variable. No puede haber más de una variable por línea.

   Como mínimo, el archivo de respuestas debe incluir las siguientes tres variables, que son obligatorias:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   Si desea que la instalación remota se lleve a cabo con otros parámetros específicos, agregue las variables opcionales que correspondan. Todas las variables que puede incluir en el archivo figuran en la siguiente tabla:

   **Variables admitidas en el archivo de respuestas como parámetros de instalación en modo silencioso para el Agente de red para Linux**

Variables admitidas en el archivo de respuestas como parámetros de instalación en modo silencioso para el Agente de red para Linux

| Nombre de la variable | Obligatoria | Descripción | Valores posibles |
|---|---|---|---|
| KLNAGENT_SERVER | Sí | Contiene el nombre del Servidor de administración. El valor puede ser un nombre de dominio completo (FQDN) o una dirección IP. | Nombre DNS o dirección IP. |
| KLNAGENT_AUTOINSTALL | Sí | Define si la instalación se realizará en modo no interactivo. | 1: Usar el modo silencioso. No se le pedirá al usuario que participe del proceso de instalación.<br><br>Otro valor: No usar el modo silencioso. Se le podría pedir al usuario que participe del proceso de instalación. |
| EULA_ACCEPTED | Sí | Determina si el usuario está de acuerdo con el Contrato de licencia de usuario final (EULA) del agente de red. Si no se define esta variable, puede entenderse que el usuario no acepta el EULA. | 1: Confirmo que he leído, entendido y aceptado completamente los términos y condiciones de este Contrato de licencia de usuario final.<br><br>Otros o no especificado: No acepto los términos del Contrato de licencia (no se realiza la instalación). |
| KLNAGENT_PROXY_USE | No | Determina si los ajustes del servidor proxy se tendrán en cuenta para conectarse al Servidor de administración. El valor predeterminado es 0. | 1: Tener en cuenta los ajustes del servidor proxy.<br><br>Otro valor: Ignorar los ajustes del servidor proxy. |
| KLNAGENT_PROXY_ADDR | No | Define la dirección del servidor proxy que se usará al conectarse con el Servidor de administración. | Nombre DNS o dirección IP. |
| KLNAGENT_PROXY_LOGIN | No | Define el nombre de usuario que se usará para identificarse ante el servidor proxy. | Cualquier nombre de usuario existente. |
| KLNAGENT_PROXY_PASSWORD | No | Define la contraseña de usuario que se usará para identificarse ante el servidor proxy. | Cualquier secuencia de caracteres alfanuméricos que el sistema operativo permita usar como contraseña. |
| KLNAGENT_VM_VDI | No | Determina si el Agente de red se instalará en una imagen que luego vaya a utilizarse para crear máquinas virtuales dinámicas. | 1: El Agente de red se instalará en una imagen con la que luego se crearán máquinas virtuales dinámicas.<br><br>Otro valor: La aplicación no se instalará en una imagen. |
| KLNAGENT_VM_OPTIMIZE | No | Determina si el Agente de red usará los ajustes de configuración optimizados para hipervisores. | 1: La configuración local predeterminada del Agente de red se modificará y se aplicarán los ajustes optimizados para hipervisores. |
| KLNAGENT_TAGS | No | Contiene la lista de etiquetas que se asignarán a la instancia del Agente de red. | Una o más etiquetas, separadas con punto y coma. |
| KLNAGENT_UDP_PORT | No | Define el puerto UDP que usará el Agente de red. El valor predeterminado es 15000. | Cualquier número de puerto. |
| KLNAGENT_PORT | No | Define el puerto no TLS que usará el Agente de red. El valor predeterminado es 14000. | Cualquier número de puerto. |

| | | | |
|---|---|---|---|
| KLNAGENT_SSLPORT | No | Define el puerto TLS que usará el Agente de red. El valor predeterminado es 13000. | Cualquier número de puerto. |
| KLNAGENT_USESSL | No | Determina si se usará el protocolo TLS para establecer la conexión. | 1 (valor predeterminado): Usar TLS.<br><br>Otro valor: No usar TLS. |
| KLNAGENT_GW_MODE | No | Determina si se usará una puerta de enlace de conexión. | 1 (valor predeterminado): Mantener la configuración existente (no se usará una puerta de enlace de conexión en la primera llamada).<br><br>2: No usar una puerta de enlace de conexión.<br><br>3: Usar una puerta de enlace de conexión. Se requiere KLNAGENT_GW_ADDRESS.<br><br>4: La instancia de Agente de red actuará como puerta de enlace de conexión en una zona desmilitarizada (DMZ). Se requiere certificado de servidor. |
| KLNAGENT_GW_ADDRESS | No | Determina la dirección de la puerta de enlace de conexión. El valor solo se tiene en cuenta cuando KLNAGENT_GW_MODE=3. | Nombre DNS o dirección IP. |
| KLNAGENT_DEVICEOWNER_REGISTRATION_START | No | Permite ejecutar la utilidad para registrar a un usuario como propietario del dispositivo tras la instalación del Agente de red. Si deshabilita esta función, el usuario no podrá registrarse como propietario del dispositivo. | 1: La utilidad para registrar al usuario como propietario del dispositivo se ejecutará tras la instalación del Agente de red.<br><br>Otro valor: deshabilitado. |

5. Descargue el paquete de instalación del Agente de red. La variable de entorno KLAUTOANSWERS, que especifica la ruta al archivo de respuesta, se pasa al comando de instalación. Ejecute uno de los siguientes comandos:

   - Para instalar el Agente de red desde un paquete RPM a un sistema operativo de 32 bits, ejecute el siguiente comando:
     `sudo KLAUTOANSWERS=< ruta al archivo de respuesta > yum install ./klnagent-< número de compilación >.i386.rpm`

   - Para instalar el Agente de red desde un paquete RPM a un sistema operativo de 64 bits, ejecute el siguiente comando:
     `sudo KLAUTOANSWERS=< ruta al archivo de respuesta > yum install ./klnagent64-< número de compilación >.x86_64.rpm`

   - Para instalar el Agente de red desde un paquete RPM en un sistema operativo de 64 bits para la arquitectura Arm, ejecute el siguiente comando:
     `sudo KLAUTOANSWERS=< ruta al archivo de respuesta > yum install ./klnagent64-< número de compilación >.aarch64.rpm`

   - Para instalar el Agente de red desde un paquete DEB a un sistema operativo de 32 bits, ejecute el siguiente comando:

```
sudo KLAUTOANSWERS=< ruta al archivo de respuesta > apt install ./klnagent_< número de compilación >_i386.deb
```

- Para instalar el Agente de red desde un paquete DEB a un sistema operativo de 64 bits, ejecute el siguiente comando:
  ```
  sudo KLAUTOANSWERS=< ruta al archivo de respuesta > apt install ./klnagent64_< número de compilación >_amd64.deb
  ```

- Para instalar el Agente de red desde un paquete DEB en un sistema operativo de 64 bits para la arquitectura Arm, ejecute el siguiente comando:
  ```
  sudo KLAUTOANSWERS=< ruta al archivo de respuesta > apt install ./klnagent64_< número de compilación >_arm64.deb
  ```

Dependiendo de la configuración del sistema operativo, también puede usar los administradores de paquetes rpm, dpkg o dnf para instalar el Agente de red.

Comenzará la instalación del Agente de red para Linux en modo silencioso. No se le pedirá al usuario que participe del proceso.

## Preparación de un dispositivo que ejecuta Astra Linux en el modo de entorno de software cerrado para la instalación del Agente de red

Antes de la instalación del Agente de red en un dispositivo que ejecuta Astra Linux en el modo de entorno de software cerrado, debe realizar dos procedimientos de preparación: el de las instrucciones a continuación y los pasos generales de preparación para cualquier dispositivo Linux.

Ejecute los comandos provistos en estas instrucciones utilizando una cuenta con privilegios de root.

*Para preparar un dispositivo que ejecuta Astra Linux en el modo de entorno de software cerrado para la instalación del Agente de red:*

1. Abra el archivo `/etc/digsig/digsig_initramfs.conf` y luego especifique la siguiente configuración:
   ```
   DIGSIG_ELF_MODE=1
   ```

2. En la línea de comandos, ejecute el siguiente comando para instalar el paquete de compatibilidad:
   ```
   apt install astra-digsig-oldkeys
   ```

3. Cree un directorio para la clave de la aplicación:
   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Coloque la clave de la aplicación en el directorio creado en el paso anterior:
   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   Si el kit de distribución de Kaspersky Security Center no incluye la clave de la aplicación kaspersky_astra_pub_key.gpg, puede descargarla haciendo clic en el vínculo: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Actualice los discos RAM:
   ```
   update-initramfs -u -k all
   ```
   Reinicie el sistema.

El dispositivo Linux está listo para la instalación del Agente de red. Puede instalar el Agente de red de forma remota, en modo interactivo o en modo silencioso.

## Instalación del Agente de red para Linux en modo interactivo

En este artículo, se describe cómo instalar el Agente de red en dispositivos Linux en modo interactivo. En este modo, los parámetros de instalación se indican paso por paso. También puede usarse un archivo de respuestas: un archivo de texto que contiene un conjunto personalizado de parámetros de instalación (variables con sus respectivos valores). El archivo de respuestas permite realizar la instalación en modo silencioso, es decir, sin involucrar al usuario.

> Si desea instalar el Agente de Red en dispositivos que utilicen el sistema operativo RED OS 7.3.4 o posterior, o MSVSPHERE 9.2 o posterior, instale el paquete libxcrypt-compat para el correcto funcionamiento del Agente de Red.

*Para instalar el Agente de red en modo interactivo:*

1. Descargue el paquete de instalación del Agente de red. Dependiendo de su distribución de Linux, ejecute uno de los siguientes comandos:

   - Para instalar el Agente de red desde un paquete RPM en un sistema operativo de 32 bits:

     ```
     # yum -i klnagent-<número de compilación>.i386.rpm
     ```

   - Para instalar el Agente de red desde un paquete RPM en un sistema operativo de 64 bits:

     ```
     # yum -i klnagent64-<número de compilación>.x86_64.rpm
     ```

   - Para instalar el Agente de red desde un paquete RPM en un sistema operativo de 64 bits para la arquitectura ARM:

     ```
     # yum -i klnagent64-<número de compilación>.aarch64.rpm
     ```

   - Para instalar el Agente de red desde un paquete DEB en un sistema operativo de 32 bits:

     ```
     # apt install ./klnagent_<número de compilación>_i386.deb
     ```

   - Para instalar el Agente de red desde un paquete DEB en un sistema operativo de 64 bits:

     ```
     # apt install ./klnagent64_<número de compilación>_amd64.deb
     ```

   - Para instalar el Agente de red desde un paquete DEB en un sistema operativo de 64 bits para la arquitectura ARM:

     ```
     # apt install ./klnagent64_<número de compilación>_arm64.deb
     ```

2. Realice la configuración del Agente de red:

   ```
   # /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. Lea el Contrato de licencia de usuario final (EULA). El texto se muestra en la ventana de la línea de comandos. Presione la barra espaciadora para ver el siguiente segmento de texto. Luego, cuando se le solicite, ingrese uno de los siguientes valores:

   - Ingrese `y` si comprende y acepta los términos del EULA.
   - Ingrese `n` si no acepta los términos del EULA. Para usar el Agente de red, debe aceptar las condiciones del EULA.
   - Ingrese `r` para volver a mostrar el EULA.

4. Ingrese el nombre DNS o la dirección IP del Servidor de administración.
5. Ingrese el número de puerto del Servidor de administración. De manera predeterminada, se utiliza el puerto 14000.
6. Ingrese el número de puerto SSL del Servidor de administración. De manera predeterminada, se utiliza el puerto 13000.
7. Ingrese `y` si desea utilizar cifrado SSL para el tráfico entre el Agente de red y el Servidor de administración. De lo contrario, ingrese `n`.
8. Seleccione una de las siguientes opciones para configurar el Agente de red:

   - `[1]`: no configurar una puerta de enlace de conexión.

     Su dispositivo no funcionará como puerta de enlace de conexión ni se conectará al Servidor de administración a través de una puerta de enlace de conexión.

   - `[2]`: no usar una puerta de enlace de conexión.

     Su dispositivo no se conectará al Servidor de administración a través de una puerta de enlace de conexión.

   - `[3]`: conectarse al Servidor mediante una puerta de enlace de conexión.

     Su dispositivo se conectará al Servidor de administración a través de una puerta de enlace de conexión.

   - `[4]`: usar como puerta de enlace de conexión.

     Su dispositivo funcionará como puerta de enlace de conexión.

El Agente de red queda instalado en el dispositivo Linux.

## Instalación local del complemento de administración de aplicaciones

*Para instalar el complemento de administración de aplicaciones:*

En el dispositivo que tiene la Consola de administración instalada, ejecute el archivo ejecutable klcfginst.exe, que se incluye en el paquete de distribución de aplicaciones.

El archivo klcfginst.exe se incluye en todas las aplicaciones que pueden administrarse por medio de Kaspersky Security Center. Un asistente facilita la instalación y no se requiere ninguna configuración manual de los parámetros.

## Instalación de aplicaciones en modo no interactivo

*Para instalar una aplicación en modo no interactivo:*

1. Abra la ventana principal de la aplicación de Kaspersky Security Center.
2. En la carpeta **Instalación remota** del árbol de consola, en la subcarpeta **Paquetes de instalación**, seleccione el paquete de instalación de la aplicación relevante o cree uno nuevo para esa aplicación.

   Los paquetes de instalación se almacenan en el Servidor de administración en la carpeta de servicios de paquetes dentro de la carpeta compartida. A cada paquete de instalación le corresponde una subcarpeta separada.

3. Abra la carpeta que almacena el paquete de instalación requerido de una de las siguientes maneras:

   - Copie en el dispositivo cliente la carpeta que corresponda al paquete de instalación relevante del Servidor de administración. A continuación, abra la carpeta copiada en el dispositivo cliente.
   - Abra desde el dispositivo cliente la carpeta compartida que equivale al paquete de instalación necesario en el Servidor de administración.

   Si la carpeta compartida está ubicada en un dispositivo con Microsoft Windows Vista instalado, seleccione el valor **Deshabilitado** para la configuración **Control de cuenta de usuario: ejecutar todos los administradores en el Modo de aprobación de administrador** (**Iniciar** → **Panel de control** → **Administración** → **Directiva de seguridad local** → **Configuración de seguridad**).

4. Según la aplicación seleccionada, realice lo siguiente:

   - Para Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers y Kaspersky Security Center, diríjase a la subcarpeta exec y ejecute el archivo ejecutable (el archivo con la extensión .exe) con la tecla /s.
   - Para otras aplicaciones Kaspersky, ejecute el archivo ejecutable (un archivo con la extensión .exe) con la tecla /s desde la carpeta abierta.

   La ejecución del archivo ejecutable con las claves `EULA=1` y `PRIVACYPOLICY=1` significa que usted leyó, comprende y acepta los términos del Contrato de licencia de usuario final y la Política de privacidad, respectivamente. También está al corriente de que sus datos serán manejados y transmitidos (incluso a otros países) como se describe en la Política de privacidad. El texto del Contrato de licencia y la Política de privacidad se incluye en el kit de distribución de Kaspersky Security Center. Aceptar las condiciones del Contrato de licencia y de la Política de privacidad es necesario para instalar la aplicación o actualizar una versión previa de la aplicación.

## Instalación de aplicaciones con paquetes independientes

Kaspersky Security Center le permite crear paquetes de instalación independientes para aplicaciones. Un paquete de instalación independiente es un archivo ejecutable que se puede encontrar en un servidor web, enviar por correo electrónico o transferir a un dispositivo cliente de algún otro modo. El archivo recibido puede ejecutarse localmente en el dispositivo cliente para instalar una aplicación sin involucrar a Kaspersky Security Center.

El Agente de red independiente para Linux tiene una dependencia opcional de la utilidad nmap. Si falta la utilidad nmap o es anterior a la versión 6.0, no se admite la funcionalidad Broadcast DHCP Discover.

*Para instalar una aplicación con un paquete de instalación independiente:*

1. Conéctese al Servidor de administración necesario.
2. En la carpeta **Instalación remota** del árbol de la consola, seleccione la subcarpeta **Paquetes de instalación**.
3. En el espacio de trabajo, seleccione el paquete de instalación de la aplicación requerida.
4. Inicie el proceso de creación de un paquete de instalación independiente usando uno de los siguientes métodos:
   - Al seleccionar **Crear un paquete de instalación independiente** en el paquete de instalación.
   - Al hacer clic en el enlace **Crear un paquete de instalación independiente** en el espacio de trabajo del paquete de instalación.

   Se inicia el asistente de creación de paquetes de instalación independiente. Siga las instrucciones del asistente.

   En el último paso del asistente, seleccione un método para transferir el paquete de instalación independiente a un dispositivo cliente.
5. Transfiera el paquete de instalación independiente al dispositivo cliente.
6. Ejecute el paquete de instalación independiente en el dispositivo cliente.

La aplicación ahora se encuentra instalada en el dispositivo cliente con la configuración especificada en el paquete independiente.

Al crear un paquete de instalación independiente, éste se publica automáticamente en el servidor web. En la lista de paquetes de instalación independiente creados se muestra un enlace para descargar el paquete independiente. De ser necesario, puede cancelar la publicación del paquete independiente seleccionado y publicarlo nuevamente en el servidor web. De forma predeterminada, se utiliza el puerto 8060 para la descarga de los paquetes de instalación independiente.

## Ajustes del paquete de instalación del Agente de red

*Para configurar un paquete de instalación del Agente de red, haga lo siguiente:*

1. En la carpeta **Instalación remota** del árbol de la consola, seleccione la subcarpeta **Paquetes de instalación**.

   De manera predeterminada, la carpeta **Instalación remota** es una subcarpeta de la carpeta **Avanzado**.
2. En el menú contextual del paquete de instalación del Agente de red, seleccione **Propiedades**.

Se abre la ventana de propiedades del paquete de instalación del Agente de red.

## General

La sección **General** muestra información general sobre el paquete de instalación:

- Nombre del paquete de instalación
- Nombre y versión de la aplicación para la que se ha creado el paquete de instalación
- Tamaño del paquete de instalación
- Fecha de creación del paquete de instalación
- Ruta a la carpeta del paquete de instalación

## Configuración

Esta sección contiene los ajustes necesarios para garantizar que el Agente de red funcione correctamente en cuanto concluya su instalación. Los ajustes de la sección solo están disponibles en dispositivos con Windows.

En el grupo de ajustes **Carpeta de destino**, puede seleccionar la carpeta del dispositivo cliente en la cual se instalará el Agente de red.

- **Instalar en la carpeta predeterminada**

  Si se selecciona esta opción, el Agente de red se instalará en la carpeta <Unidad>:\Archivos de programa\Kaspersky Lab\NetworkAgent. Si esta carpeta no existe, se la creará automáticamente.

  Esta opción está seleccionada de forma predeterminada.

- **Instalar en la carpeta especificada**

  Si se selecciona esta opción, el Agente de red se instalará en la carpeta especificada en el campo de entrada.

El siguiente grupo de ajustes permite especificar una contraseña para la tarea de desinstalación remota del Agente de red:

- **Utilizar contraseña de desinstalación**

  Si habilita esta opción, podrá hacer clic en el botón **Modificar** para ingresar la contraseña de desinstalación (solo disponible para el Agente de red en dispositivos con sistemas operativos Windows).

  Esta opción está deshabilitada de forma predeterminada.

- **Estado**

  Estado de la contraseña: **Contraseña establecida** o **Contraseña no establecida**.

  De manera predeterminada, esta contraseña no está establecida.

- **Evitar que el servicio del Agente de red se detenga o se elimine sin autorización e impedir cambios en su configuración**

  Cuando esta opción está habilitada, una vez que el Agente de red se encuentre instalado en un dispositivo administrado, no se lo podrá eliminar ni reconfigurar a menos que se tengan los privilegios necesarios. El servicio del Agente de red no se podrá detener. Esta opción no tiene efecto en los controladores de dominio.

  Habilite esta opción para proteger el Agente de red en estaciones de trabajo operadas con derechos de administrador local.

  Esta opción está deshabilitada de forma predeterminada.

- **Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes**

  Si esta opción está habilitada, todas las actualizaciones y parches descargados para el Servidor de administración, el Agente de red, la Consola de administración y el Servidor de MDM para iOS se instalarán automáticamente.

  Si se deshabilita esta opción, las actualizaciones y los parches que se descarguen se instalarán únicamente después de que su estado se cambie a *Aprobado*. Las actualizaciones y los parches con el estado *Sin definir* no se instalarán.

  Esta opción está activada de forma predeterminada.

## Conexión

En esta sección, puede configurar la conexión del Agente de red al Servidor de administración. Para establecer una conexión, pueden utilizarse los protocolos SSL o UDP. Defina los siguientes ajustes para configurar la conexión:

- **Servidor de administración**

  Dirección del dispositivo en el que se encuentra instalado el Servidor de administración.

- **Puerto**

  Número de puerto que se utilizará para la conexión.

- **Puerto SSL**

  Número de puerto que se utilizará para la conexión mediante el protocolo SSL.

- **Usar certificado del Servidor**

  Si se habilita esta opción, para autenticar el acceso del Agente de red al Servidor de administración, se usará el archivo del certificado seleccionado al hacer clic en el botón **Examinar**.

  Si se deshabilita esta opción, el archivo del certificado se obtendrá del Servidor de administración la primera vez que el Agente de red se conecte a la dirección especificada en el campo **Dirección del Servidor**.

  No recomendamos que deshabilite esta opción: no se considera seguro que el Agente de red obtenga el certificado del Servidor de administración automáticamente al establecer conexión.

  Esta casilla está activada de manera predeterminada.

- **Usar SSL**

  Si se habilita esta opción, la conexión al Servidor de administración se establecerá a través de un puerto seguro utilizando el protocolo SSL.

  Esta opción está deshabilitada de forma predeterminada. Recomendamos no deshabilitar esta opción; de lo contrario, la conexión quedará desprotegida.

- **Usar puerto UDP**

  Si se habilita esta opción, el Agente de red se conectará al Servidor de administración a través de un puerto UDP. Esto permite administrar los dispositivos cliente y recibir información sobre ellos.

  El puerto UDP deberá estar abierto en los dispositivos administrados en los que se instale el Agente de red. Por lo tanto, recomendamos no deshabilitar esta opción.

  Esta opción está activada de forma predeterminada.

- **Número de puerto UDP**

  En este campo, puede ingresar el número de puerto que se usará para conectar el Agente de red al Servidor de administración mediante el protocolo UDP.

  El número de puerto UDP predeterminado es 15000.

- Abrir los puertos del Agente de red en el Firewall de Microsoft Windows

  Cuando se habilita esta opción, se agregan los puertos que el Agente de red utiliza a la lista de exclusiones del Firewall de Microsoft Windows.

  Esta opción está activada de forma predeterminada.

- Usar servidor proxy

  Si esta opción está habilitada, especifique los parámetros del servidor proxy:

  - **Dirección del servidor proxy**
  - **Puerto del servidor proxy**

  Si su servidor proxy requiere autenticación, habilite la opción **Autenticación del servidor proxy** y especifique el **Nombre de usuario** y la **Contraseña** de la cuenta con la que se establece la conexión con el servidor proxy. Le recomendamos que utilice las credenciales de una cuenta que solamente tenga los privilegios mínimos necesarios para completar la autenticación ante el servidor proxy.

Por motivos de compatibilidad, no se recomienda especificar la configuración de la conexión del proxy en la configuración del paquete de instalación del Agente de red.

## Avanzado

La sección **Avanzado** le permite configurar cómo se usará la puerta de enlace de conexión. Las opciones disponibles son las siguientes:

- Utilizar el Agente de red como puerta de enlace de conexión en una zona desmilitarizada (DMZ) para conectarse al Servidor de administración, comunicarse con este y mantener seguros los datos en el Agente de red durante la transmisión de datos.

- Conectarse al Servidor de administración a través de una puerta de enlace de conexión para reducir la cantidad de conexiones al Servidor de administración. Si elige esta opción, ingrese la dirección del dispositivo que actuará como puerta de enlace de conexión en el campo **Dirección de la puerta de enlace de conexión**.

- Configurar la conexión para una infraestructura de escritorios virtuales (VDI) si su red contiene máquinas virtuales. Para esto, haga lo siguiente:

  - **Habilitar modo dinámico para VDI**

    Si habilita esta opción, se habilitará un modo dinámico para infraestructuras de escritorios virtuales (VDI) para el Agente de red instalado en una máquina virtual.

    Esta opción está deshabilitada de forma predeterminada.

  - **Optimizar la configuración para VDI**

    Si habilita esta opción, se deshabilitarán las siguientes características de la configuración del Agente de red:

    - Recopilación de información acerca del software instalado
    - Recopilación de información acerca del hardware
    - Recopilación de información acerca de las vulnerabilidades detectadas
    - Recopilación de información acerca de las actualizaciones necesarias

    Esta opción está deshabilitada de forma predeterminada.

- **Permitir la ejecución de la utilidad de registro de usuario luego de la instalación del Agente de red**

  Si esta opción está habilitada, la utilidad de registro del usuario como propietario del dispositivo se ejecutará después de la instalación del Agente de red. Esta opción está deshabilitada de forma predeterminada.

## Componentes adicionales

En esta sección, puede seleccionar los componentes adicionales que desee instalar junto con el Agente de red.

## Etiquetas

La sección **Etiquetas** muestra una lista de palabras claves (etiquetas) que se pueden agregar a los dispositivos cliente tras la instalación del Agente de red. Puede agregar etiquetas nuevas a la lista, así como eliminar las etiquetas existentes o cambiarles el nombre.

Si la casilla junto a una etiqueta está marcada, cuando se instale el Agente de red, la etiqueta correspondiente se agregará a los dispositivos administrados de manera automática.

Si la casilla junto a una etiqueta no está marcada, la etiqueta no se agregará automáticamente a los dispositivos administrados durante la instalación del Agente de red. De ser necesario, podrá agregar esa etiqueta manualmente a los dispositivos pertinentes.

Si elimina una etiqueta de la lista, se la eliminará automáticamente de todos los dispositivos a los que haya sido agregada.

### Historial de revisiones

En esta sección, puede ver el historial de revisiones del paquete de instalación. Puede comparar las distintas revisiones, ver revisiones específicas, guardar revisiones en un archivo, agregar descripciones a las revisiones y modificar las descripciones existentes.

La siguiente tabla detalla los ajustes disponibles para el paquete de instalación del Agente de red según el sistema operativo.

Ajustes del paquete de instalación del Agente de red

| Sección de propiedades | Windows | Mac | Linux |
|---|---|---|---|
| **General** | ✓ | ✓ | ✓ |
| **Configuración** | ✓ | — | — |
| **Conexión** | ✓ | ✓ (excepto las opciones **Abrir los puertos del Agente de red en el Firewall de Microsoft Windows** y **Utilizar solo detección automática de servidor proxy**) | ✓ (excepto las opciones **Abrir los puertos del Agente de red en el Firewall de Microsoft Windows** y **Utilizar solo detección automática de servidor proxy**) |
| **Avanzado** | ✓ | ✓ | ✓ |
| **Componentes adicionales** | ✓ | ✓ | ✓ |
| **Etiquetas** | ✓ | ✓ (excepto las reglas de etiquetado automático) | ✓ (excepto las reglas de etiquetado automático) |
| **Historial de revisiones** | ✓ | ✓ | ✓ |

### Ver la Política de privacidad

La Política de privacidad está disponible en línea en https://latam.kaspersky.com/products-and-services-privacy-policy; también está disponible sin conexión. Tendrá oportunidad de leer esta política antes de instalar el Agente de red, por ejemplo.

*Para leer la Política de privacidad sin conexión:*

1. Inicie el instalador de Kaspersky Security Center.
2. En la ventana del instalador, vaya al vínculo **Extraer paquetes de instalación**.
3. En la lista que se abre, seleccione Agente de red de Kaspersky Security Center y luego haga clic en **Siguiente**.

El archivo privacy_policy.txt aparece en su dispositivo, en la carpeta que especificó, en la subcarpeta NetAgent.

## Despliegue de los sistemas de administración de dispositivos móviles

En esta sección, se describe el proceso para desplegar los sistemas que le permitirán administrar dispositivos móviles a través de los protocolos de Kaspersky Endpoint Security y MDM para iOS.

# Despliegue de un sistema de administración para el protocolo MDM para iOS

Kaspersky Security Center le permite administrar dispositivos móviles que funcionan con iOS. Los dispositivos móviles MDM con iOS son dispositivos móviles iOS conectados a un servidor de MDM para iOS y administrados por un Servidor de administración.

Siga estos pasos a fin de conectar dispositivos móviles a un servidor de MDM para iOS:

1. El administrador instala el servidor de MDM para iOS.

2. El administrador obtiene un certificado del Servicio de notificaciones push de Apple (Recibir un certificado de APNs, https://support.kaspersky.com/help/KSMM/4.1/en-US/64900.htm).

   El certificado de APNs permite que el Servidor de administración se conecte con el servidor APNs para enviar notificaciones push a dispositivos móviles MDM con iOS.

3. El administrador instala el certificado de APNs en el Servidor de MDM para iOS.

4. El administrador crea un perfil de MDM para iOS para el usuario del dispositivo móvil iOS.

   El perfil de MDM para iOS incluye una colección de ajustes para conectar dispositivos móviles iOS al Servidor de administración.

Después de instalar el perfil de MDM para iOS y de sincronizar el dispositivo MDM con iOS con el Servidor de administración, el dispositivo se muestra en la carpeta **Dispositivos móviles**, que es una subcarpeta de la carpeta **Administración de dispositivos móviles** del árbol de consola.

## Instalación del Servidor de MDM para iOS

*Para instalar el servidor de MDM para iOS en un dispositivo local:*

1. Ejecute el archivo ejecutable setup.exe.

   Se abre una ventana y se le solicita que seleccione las aplicaciones de Kaspersky que desea instalar.

   En la ventana de selección de aplicaciones, haga clic en el vínculo **Instalar el Servidor de MDM para iOS** para ejecutar el Asistente de instalación del Servidor de MDM para iOS.

2. Seleccione una carpeta de destino.

   La carpeta de destino predeterminada es <Unidad>:\Archivos de programa\Kaspersky Lab\Mobile Device Management for iOS. Si la carpeta no existe, se crea automáticamente durante la instalación. Es posible cambiar la carpeta de destino usando el botón **Examinar**.

3. En la ventana **Especifique los parámetros de conexión al Servidor de MDM para iOS** del Asistente, en el campo **Puerto externo para conectarse al servicio MDM para iOS**, especifique un puerto externo para la conexión de dispositivos móviles al servicio MDM para iOS.

   Los dispositivos móviles usan el puerto externo 5223 para comunicarse con el servidor de APNs. Asegúrese de que el puerto 5223 esté abierto en el firewall para la conexión con el intervalo de direcciones 17.0.0.0/8.

   El Puerto 443 se utiliza para la conexión con el Servidor de MDM para iOS de forma predeterminada. Si el puerto 443 ya está siendo utilizado por otro servicio o aplicación, puede ser remplazado con, por ejemplo, el puerto 9443.

   El Servidor de MDM para iOS usa el puerto externo 2197 para enviar notificaciones al servidor de APNs.

   Los servidores de APNs se ejecutan en el modo de balance de cargas. Los dispositivos móviles no siempre se conectan a las mismas direcciones IP para recibir notificaciones. El rango de direcciones 17.0.0.0/8 está reservado para Apple, motivo por el que se recomienda que especifique este rango completo como un rango permitido en la configuración del Firewall.

4. Si desea configurar manualmente puertos de interacción para componentes de la aplicación, seleccione la opción **Configure los puertos locales manualmente** y, a continuación, especifique valores para la siguiente configuración:

   - **Puerto usado para conectarse con el Agente de red**. En este campo, especifique un puerto para conectar el servicio MDM para iOS al Agente de red. El número de puerto predeterminado es 9799.
   - **Puerto local para conectarse al servicio MDM para iOS**. En este campo, especifique un puerto local para conectar el Agente de red al servicio MDM para iOS. El número de puerto predeterminado es 9899.

   Se recomienda utilizar los valores predeterminados.

5. En la ventana **Dirección externa del Servidor de dispositivos móviles** del Asistente, en **Dirección web para la conexión remota con el Servidor de dispositivo móvil**, especifique la dirección del dispositivo cliente en el que se instalará Servidor de MDM para iOS.

   Esta dirección se usará para conectar dispositivos móviles administrados al servicio MDM para iOS. Este dispositivo cliente debe estar disponible para establecer la conexión de los dispositivos MDM con iOS.

   Puede especificar la dirección de un dispositivo cliente en cualquiera de los siguientes formatos:

   - FQDN del dispositivo (por ejemplo, mdm.example.com)
   - Nombre NetBIOS del dispositivo

   Evite agregar el esquema URL y el número de puerto a la cadena de dirección; estos valores se agregarán automáticamente.

Cuando el Asistente finaliza, el Servidor de MDM para iOS estará instalado en el dispositivo local. El Servidor de MDM para iOS se muestra en la carpeta **Administración de dispositivos móviles** del árbol de consola.

## Instalación del Servidor de MDM para iOS en modo no interactivo

Kaspersky Security Center permite instalar el Servidor de MDM para iOS en un dispositivo local en el modo no interactivo, es decir, sin entrada interactiva de la configuración de instalación.

*Para instalar el Servidor de MDM para iOS en un dispositivo local en modo no interactivo:*

1. Lea el Contrato de licencia de usuario final. Use el comando a continuación únicamente si comprende y acepta los términos del Contrato de licencia de usuario final.

2. Ejecute el siguiente comando:

   ```
   .\exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 <parámetros_de_instalación>"
   ```

   donde `parámetros_de_instalación` es una lista de parámetros y sus valores correspondientes separados por un espacio (`PROP1=PROP1VAL PROP2=PROP2VAL`). El archivo setup.exe se ubica en la carpeta Servidor, que es parte del kit de distribución de Kaspersky Security Center.

En la siguiente tabla se enumeran los nombres y valores posibles de las opciones de parámetros que pueden usarse al instalar el Servidor de MDM para iOS en modo no interactivo. La configuración se puede especificar en cualquier orden conveniente.

Parámetros de instalación del Servidor de MDM para iOS en modo no interactivo

| Nombre del parámetro | Descripción del parámetro | Valores disponibles |
|---|---|---|
| EULA | Aceptación de los términos del Contrato de licencia de usuario final. Este parámetro es obligatorio. | • 1: he leído, comprendo y acepto en su totalidad los términos del Contrato de licencia de usuario final.<br>• Otro valor o ningún valor: no acepto los términos del Contrato de licencia (no se realizará la instalación). |
| DONT_USE_ANSWER_FILE | Usar o no un archivo XML con la configuración de instalación del Servidor de MDM para iOS.<br>El archivo XML se incluye en el paquete de instalación o se almacena en el Servidor de administración. No tiene que especificar una ruta adicional al archivo.<br>Este parámetro es obligatorio. | • 1: No utilice el archivo XML con los parámetros.<br>• Otro valor o sin valor: utilice el archivo de XML con los parámetros. |
| INSTALLDIR | Carpeta de instalación del Servidor de MDM para iOS.<br>Este parámetro es opcional. | Valor de cadena, por ejemplo, `INSTALLDIR=\"C:\install\"` |
| CONNECTORPORT | Puerto local para conectar el servicio MDM para iOS al Agente de red.<br>El número de puerto predeterminado es 9799.<br>Este parámetro es opcional. | Valor numérico. |
| LOCALSERVERPORT | Puerto local para conectar un Agente de red al servicio MDM para iOS.<br>El número de puerto predeterminado es el 9899.<br>Este parámetro es opcional. | Valor numérico. |
| EXTERNALSERVERPORT | Puerto para conectar un dispositivo al Servidor de MDM para iOS.<br>El número de puerto predeterminado es 443.<br>Este parámetro es opcional. | Valor numérico. |
| EXTERNAL_SERVER_URL | La dirección externa del dispositivo cliente en el cual se debe instalar el Servidor de MDM para iOS. Esta dirección se usará para conectar dispositivos móviles administrados al servicio MDM para iOS. El dispositivo cliente debe estar disponible para la conexión a través de MDM para iOS.<br>La dirección no debe incluir el esquema de la URL y el número del puerto ya que estos valores se agregarán automáticamente.<br>Este parámetro es opcional. | • FQDN del dispositivo (por ejemplo, mdm.example.com)<br>• Nombre NetBIOS del dispositivo<br>• Dirección IP del dispositivo |

| Nombre del parámetro | Descripción del parámetro | Valores disponibles |
|---|---|---|
| WORKFOLDER | Carpeta de trabajo del Servidor de MDM para iOS.<br>Si no se especifica ninguna carpeta de trabajo, los datos se escribirán en la carpeta predeterminada.<br>Este parámetro es opcional. | Valor de cadena, por ejemplo, `WORKFOLDER=\"C:\work\"` |
| MTNCY | Uso de Servidor de MDM para iOS por parte de varios servidores virtuales.<br>Este parámetro es opcional. | • 1: el Servidor de MDM para iOS será utilizado por varios Servidores de administración virtuales.<br>• Otro valor o ningún valor: el Servidor de MDM para iOS no será utilizado por varios Servidores de administración virtuales. |

Ejemplo:

```
\exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1 EXTERNALSERVERPORT=9443 EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

Los parámetros de instalación del servidor de MDM para iOS se detallan en la sección "Instalación del servidor de MDM para iOS".

## Escenarios de despliegue del Servidor de MDM para iOS

El número de copias del Servidor de MDM para iOS que se debe instalar se puede seleccionar según el hardware disponible o el número total de dispositivos móviles cubiertos.

Tenga en cuenta que el número máximo recomendado de dispositivos móviles para una instalación sola de Kaspersky Device Management for iOS es 50 000 como máximo. A fin de reducir la carga, el grupo completo de dispositivos se puede distribuir entre varios servidores que tengan instalado el Servidor de MDM para iOS.

La autenticación de los dispositivos MDM con iOS se realiza a través de certificados de usuario (cualquier perfil instalado en un dispositivo contiene el certificado del propietario del dispositivo). Así, existen dos esquemas de despliegue para el Servidor de MDM para iOS:

- Esquema simplificado
- Esquema de despliegue para usar la delegación restringida de Kerberos (KCD)

## Esquema de despliegue simplificado

Cuando el Servidor de MDM para iOS se ha instalado según el esquema de despliegue simplificado, los dispositivos móviles se conectan al servicio web de MDM para iOS directamente. En este caso, los certificados de usuario emitidos por el Servidor de administración solo se pueden aplicar para la autenticación de dispositivos. La integración con la infraestructura de claves públicas (PKI) es imposible para los certificados de usuario.

## Esquema de despliegue para usar la delegación restringida de Kerberos (KCD)

Para usar el esquema de despliegue con la delegación restringida de Kerberos (KCD), se deben cumplir los siguientes requisitos:

- El Servidor de administración y el Servidor de MDM para iOS se encuentran en la red interna de la organización.
- Se está utilizando un proxy inverso compatible con KCD.

Este esquema de despliegue permite lo siguiente:

- Integración con el proxy inverso compatible con KCD
- Uso de KCD para autenticación de dispositivos móviles
- Integración con PKI para aplicar certificados de usuario

Si elige usar este esquema de despliegue, debe hacer lo siguiente:

- En la Consola de administración, en la configuración del servicio web de MDM para iOS, seleccione la casilla **Asegurar compatibilidad con la delegación restringida de Kerberos**.
- Como certificado para el servicio web de MDM para iOS, especifique el certificado personalizado que se definió cuando el servicio web de MDM para iOS se publicó en el proxy inverso.
- Los certificados de usuario para dispositivos iOS deben ser emitidos por la Entidad de certificación (CA) del dominio. Si el dominio contiene varias CA originales, los certificados de usuario debe emitirlos la CA que se especificó cuando el servicio web de MDM para iOS se publicó en el proxy inverso.

  Se puede asegurar de que el certificado cliente (certificado de usuario) se realice conforme a este requisito de emisión de CA usando uno de los métodos siguientes:

  - Especifique el certificado de usuario en el Asistente para crear un nuevo perfil de MDM para iOS y en el Asistente de instalación de certificados.
  - Integre el Servidor de administración con PKI del dominio y defina el parámetro correspondiente en las reglas para la emisión de certificados:

    1. En el árbol de consola, expanda la carpeta **Administración de dispositivos móviles** y seleccione la subcarpeta **Certificados**.
    2. En el espacio de trabajo de la carpeta **Certificados**, haga clic en el botón **Configurar reglas de emisión de certificados** para abrir la ventana **Reglas de emisión de certificados**.
    3. En la sección **Integración con PKI**, configure la integración con la Infraestructura de clave pública.
    4. En la sección **Emisión de certificados para dispositivos móviles**, especifique el origen de los certificados.

A continuación se muestra un ejemplo de instalación de la delegación restringida de Kerberos (KCD) con las siguientes suposiciones:

- El servicio web de MDM para iOS se está ejecutando en el puerto 443.
- El nombre del dispositivo con el proxy inverso es firewall.mydom.local.
- El nombre del dispositivo con el servicio web de MDM para iOS es iosmdm.mydom.local.
- El nombre de publicación externa del servicio web de MDM para iOS es iosmdm.mydom.local.

## Nombre principal de servicio para http/iosmdm.mydom.local

En el dominio, tiene que registrar el nombre principal de servicio (SPN) en el dispositivo con el servicio web de MDM para iOS (iosmdm.mydom.local):

```
setspn -a http/iosmdm.mydom.local iosmdm
```

## Configuración de las propiedades del dominio del dispositivo con el proxy inverso (firewall.mydom.local)

Para delegar el tráfico, delegue el dispositivo con el proxy inverso (firewall.mydom.local) al servicio que es definido por SPN (http/iosmdm.mydom.local).

*Para delegar el dispositivo con el proxy inverso al servicio definido por SPN (http/iosmdm.mydom.local), el administrador debe realizar las siguientes acciones:*

1. En el complemento de Microsoft Management Console denominado "Usuarios y equipos de Active Directory", seleccione el dispositivo con el proxy inverso instalado (firewall.mydom.local).

2. En las propiedades del dispositivo, en la pestaña **Delegación**, configure la opción **Confiar este equipo para delegación para un servicio especificado únicamente** en **Usar cualquier protocolo de autenticación**.

3. Agregue el SPN (http/iosmdm.mydom.local) a los **Servicios en los cuales esta cuenta puede presentar credenciales delegadas**.

## Certificado especial (personalizado) para el servicio web publicado (iosmdm.mydom.global)

Tiene que emitir un certificado especial (personalizado) para el servicio web de MDM para iOS en FQDN iosmdm.mydom.global y especificar que reemplaza al certificado predeterminado en la configuración del servicio web de MDM para iOS en la Consola de administración.

Tenga en cuenta que el contenedor del certificado (archivo con la extensión p12 o pfx) también debe contener una cadena de certificados de origen (claves públicas).

## Publicación del servicio web de MDM para iOS en el proxy inverso

En el proxy inverso, para el tráfico que va desde un dispositivo móvil al puerto 443 de iosmdm.mydom.global, tiene que configurar KCD en SPN (http/iosmdm.mydom.local) usando el certificado emitido para FQDN (iosmdm.mydom.global). Tenga en cuenta que la publicación y el servicio web publicado deben compartir el mismo certificado del servidor.

## Recepción de un certificado de APNs

> Si ya tiene un certificado de APNs, considere renovarlo en lugar de crear uno nuevo. Cuando reemplaza el certificado de APNs existente por uno recién creado, el Servidor de administración pierde la capacidad de administrar los dispositivos móviles iOS conectados actualmente.

Cuando se crea la solicitud de firma de certificado (CSR) en el primer paso del Asistente de certificados de APNs, la clave privada de la misma se almacena en la memoria RAM del dispositivo. Por lo tanto, se deben completar todos los pasos del Asistente dentro de una misma sesión de la aplicación.

*Para recibir un certificado de APNs:*

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Servidores de dispositivos móviles**.

2. En el espacio de trabajo de la carpeta **Servidores de dispositivos móviles**, seleccione un Servidor de MDM para iOS.

3. En el menú contextual del Servidor de MDM para iOS, seleccione **Propiedades**.

   Se abre la ventana de propiedades del Servidor de MDM para iOS.

4. En la ventana de propiedades del Servidor de MDM para iOS, seleccione la sección **Certificados**.

5. En la sección **Certificados**, en el bloque de configuraciones **Certificado de Apple Push Notification**, haga clic en el botón **Solicitar nuevo**.

   Se iniciará el Asistente de recepción de certificados de APNs y se abrirá la ventana **Solicitar nuevo**.

6. Cree una solicitud de firma de certificado (denominada, en adelante, CSR). Para hacerlo, realice las siguientes acciones:

   a. Haga clic en el botón **Crear CSR**.

   b. En la ventana **Crear CSR** que se abre, especifique un nombre para su solicitud, el nombre de su empresa y de su departamento, y su ciudad, región y país.

   c. Haga clic en el botón **Guardar** y especifique un nombre para el archivo en el que se guardará CSR.

   La clave privada del certificado se guardará en la memoria del dispositivo.

7. Use su CompanyAccount para enviar el archivo con CSR que ha creado a Kaspersky para su firma.

   > La firma de su CSR solo estará disponible después de cargar una clave en el portal de CompanyAccount que le permita usar la Administración de dispositivos móviles.

   Después de procesar su solicitud en línea, recibirá un archivo CSR firmado por Kaspersky.

8. Envíe el archivo CSR firmado al sitio web de Apple Inc. mediante un ID de Apple aleatorio.

   Le recomendamos que evite usar un ID de Apple personal. Cree un ID de Apple específico para usarlo como corporativo. Después de haber creado un ID de Apple, vincúlelo con el buzón de correo de la organización, no con el buzón de correo de un empleado.

   Después de procesar su CSR en Apple Inc., recibirá la clave pública del certificado de APNs. Guarde el archivo en disco.

9. Exporte el certificado de APNs junto con la clave privada creada al generar CSR, en formato de archivo PFX. Para hacerlo, realice los siguientes pasos:

   a. En la ventana **Solicitar un nuevo certificado de APNs**, haga clic en el botón **Completar CSR**.

   b. En la ventana **Abrir**, seleccione un archivo con la clave pública del certificado recibido de Apple Inc. como consecuencia del procesamiento de CSR y, luego, haga clic en el botón **Abrir**.

      Se inicia el proceso de exportación del certificado.

   c. En la ventana siguiente, indique la contraseña de clave privada y haga clic en **Aceptar**.

      Esta contraseña se utilizará para la instalación del certificado de APNs en el Servidor de MDM para iOS.

   d. En la ventana **Guardar certificado de APNs**, especifique el nombre de archivo para el certificado de APNs, seleccione la carpeta y haga clic en **Guardar**.

Las claves privada y pública del certificado se combinan, y el certificado de APNs se guarda en formato PFX. Luego de esto, puede instalar el certificado de APNs en el Servidor de MDM para iOS.

## Renovación de un certificado de APNs

*Para renovar un certificado de APNs:*

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Servidores de dispositivos móviles**.

2. En el espacio de trabajo de la carpeta **Servidores de dispositivos móviles**, seleccione un Servidor de MDM para iOS.

3. En el menú contextual del Servidor de MDM para iOS, seleccione **Propiedades**.

   Se abre la ventana de propiedades del Servidor de MDM para iOS.

4. En la ventana de propiedades del Servidor de MDM para iOS, seleccione la sección **Certificados**.

5. En la sección **Certificados**, en el bloque de opciones **Certificado de Apple Push Notification**, haga clic en el botón **Renovar**.

   Se inicia el Asistente de renovación de certificados de APNs, y se abre la ventana **Renovar certificado de APNs**.

6. Cree una solicitud de firma de certificado (denominada, en adelante, CSR). Para hacerlo, realice las siguientes acciones:

   a. Haga clic en el botón **Crear CSR**.

   b. En la ventana **Crear CSR** que se abre, especifique un nombre para su solicitud, el nombre de su empresa y de su departamento, y su ciudad, región y país.

   c. Haga clic en el botón **Guardar** y especifique un nombre para el archivo en el que se guardará CSR.

   La clave privada del certificado se guardará en la memoria del dispositivo.

7. Use su CompanyAccount para enviar el archivo con CSR que ha creado a Kaspersky para su firma.

   > La firma de su CSR solo estará disponible después de cargar una clave en el portal de CompanyAccount que le permita usar la Administración de dispositivos móviles.

   Después de procesar su solicitud en línea, recibirá un archivo CSR firmado por Kaspersky.

8. Envíe el archivo CSR firmado al sitio web de Apple Inc. mediante un ID de Apple aleatorio.

   > Le recomendamos que evite usar un ID de Apple personal. Cree un ID de Apple específico para usarlo como corporativo. Después de haber creado un ID de Apple, vincúlelo con el buzón de correo de la organización, no con el buzón de correo de un empleado.

   Después de procesar su CSR en Apple Inc., recibirá la clave pública del certificado de APNs. Guarde el archivo en disco.

9. Solicite la clave pública del certificado. Para hacerlo, realice las siguientes acciones:

   a. Vaya al portal de certificados push de Apple. Para iniciar sesión en el portal, use la Id. de Apple recibida en la solicitud inicial del certificado.

   b. En la lista de certificados, seleccione el certificado cuyo nombre APSP (en formato "APSP: <número>") coincide con el nombre APSP del certificado utilizado por el Servidor de MDM para iOS y haga clic en el botón **Renovar** ("Renovar").

      El certificado de APNs se renueva.

   c. Guarde el certificado creado en el portal.

10. Exporte el certificado de APNs junto con la clave privada creada al generar CSR, en formato de archivo PFX. Para ello, realice las siguientes acciones:

    a. En la ventana **Renovar certificado de APNs**, haga clic en el botón **Completar CSR**.

    b. En la ventana **Abrir**, seleccione un archivo con la clave pública del certificado recibido de Apple Inc. como consecuencia del procesamiento de CSR, y presione el botón **Abrir**.

       Se iniciará el proceso de exportación del certificado.

    c. En la ventana siguiente, indique la contraseña de clave privada y haga clic en **Aceptar**.

       Esta contraseña se utilizará para la instalación del certificado de APNs en el Servidor de MDM para iOS.

    d. En la ventana **Renovar certificado de APNs** que se abre, especifique el nombre de archivo para el certificado de APNs, seleccione la carpeta y haga clic en **Guardar**.

Las claves privada y pública del certificado se combinan, y el certificado de APNs se guarda en formato PFX.

## Configuración de un certificado de reserva de Servidor de MDM para iOS

La funcionalidad del Servidor de MDM para iOS le permite emitir un certificado de reserva. Este certificado está diseñado para su uso en perfiles de MDM para iOS, para garantizar un cambio sin problemas de los dispositivos iOS administrados después de que expire el certificado del Servidor de MDM para iOS.

Si su Servidor de MDM para iOS utiliza un certificado predeterminado emitido por Kaspersky, puede emitir un certificado de reserva (o especificar su propio certificado personalizado como reserva) antes de que expire el certificado del Servidor de MDM para iOS. De forma predeterminada, el certificado de reserva se emite automáticamente 60 días antes de la expiración del certificado del Servidor de MDM para iOS. El certificado de reserva del Servidor de MDM para iOS se convierte en el certificado principal inmediatamente después de la expiración del certificado del Servidor de MDM para iOS. La clave pública se distribuye a todos los dispositivos administrados a través de perfiles de configuración, por lo que no tiene que transmitirla manualmente.

*Para emitir un certificado de reserva del Servidor de MDM para iOS o especificar un certificado de reserva personalizado:*

1. En el árbol de la consola, en la carpeta **Administración de dispositivos móviles**, seleccione la subcarpeta **Servidores de dispositivos móviles**.

2. En la lista de Servidores de dispositivos móviles, seleccione el Servidor de MDM para iOS correspondiente y, en el panel derecho, haga clic en el botón **Configurar el Servidor de MDM para iOS**.

3. En la ventana de configuración del Servidor de MDM para iOS que se abre, seleccione la sección **Certificados**.

4. En el bloque de configuraciones **Certificado de reserva**, haga uno de los siguientes:

   - Si planea continuar usando un certificado autofirmado (es decir, el emitido por Kaspersky), siga estos pasos:

     a. Haga clic en el botón **Emitir**.

     b. En la ventana **Fecha de activación** que se abre, seleccione una de las dos opciones para la fecha en que se debe aplicar el certificado de reserva:

        - Si desea aplicar el certificado de reserva en el momento de la expiración del certificado actual, seleccione la opción **Cuando caduque el certificado actual**.

        - Si desea aplicar el certificado de reserva antes de que caduque el certificado actual, seleccione la opción **Tras este período (días)**. En el campo de entrada junto a esta opción, especifique la duración del período después del cual el certificado de reserva debe reemplazar al certificado actual.

        > El período de validez del certificado de reserva que especifique no puede exceder el período de validez del certificado actual del Servidor de MDM para iOS.

     c. Haga clic en el botón **Aceptar**.

     Se emite el certificado de reserva para el Servidor de MDM para iOS.

   - Si planea utilizar un certificado personalizado emitido por su autoridad de certificación, siga estos pasos:

     a. Haga clic en el botón **Agregar**.

     b. En la ventana del Explorador de archivos que se abre, especifique un archivo de certificado en formato PEM, PFX o P12, que está almacenado en su dispositivo, y luego haga clic en el botón **Abrir**.

     Su certificado personalizado se especifica como el certificado de reserva del Servidor de MDM para iOS.

Tiene un certificado de reserva del Servidor de MDM para iOS especificado. Los detalles del certificado de reserva se muestran en el bloque de configuración **Certificado de reserva** (nombre del certificado, nombre del emisor, fecha de vencimiento y la fecha en que se debe aplicar el certificado de reserva, si corresponde).

## Instalación de un certificado de APNs en un Servidor de MDM para iOS

Después de haber recibido el certificado de APNs, debe instalarlo en el Servidor de MDM para iOS.

*Para instalar el certificado de APNs en el Servidor de MDM para iOS:*

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Servidores de dispositivos móviles**.

2. En el espacio de trabajo de la carpeta **Servidores de dispositivos móviles**, seleccione un Servidor de MDM para iOS.

3. En el menú contextual del Servidor de MDM para iOS, seleccione **Propiedades**.

   Se abre la ventana de propiedades del Servidor de MDM para iOS.

4. En la ventana de propiedades del Servidor de MDM para iOS, seleccione la sección **Certificados**.

5. En la sección **Certificados**, en el bloque de opciones **Certificado de Apple Push Notification**, haga clic en el botón **Instalar**.

6. Seleccione el archivo PFX que incluye el certificado de APNs.

7. Escriba la contraseña de la clave privada que se especificó al exportar el certificado de APNs.

El certificado de APNs se instalará en el Servidor de MDM para iOS. Los detalles del certificado se mostrarán en la ventana de propiedades del Servidor de MDM para iOS en la sección **Certificados**.

## Configuración del acceso al servicio de Apple Push Notification

Para asegurar un correcto funcionamiento del servicio web de MDM para iOS y las respuestas oportunas de los dispositivos móviles a los comandos del administrador, tiene que especificar un certificado del Servicio de Apple Push Notification (denominado en lo sucesivo certificado de APNs) en la configuración del Servidor de MDM para iOS.

Al interactuar con Apple Push Notification (denominado en lo sucesivo APNs), el servicio web de MDM para iOS se conecta a la dirección externa api.push.apple.com a través del puerto 2197 (saliente). Por lo tanto, el servicio web de MDM para iOS requiere acceso al puerto TCP 2197 para el rango de direcciones 17.0.0.0/8. Desde el dispositivo iOS el acceso es al puerto TCP 5223 para el rango de direcciones 17.0.0.0/8.

Si tiene la intención de acceder a APNs desde el lado del servicio web de MDM para iOS a través de un servidor proxy, debe realizar las siguientes acciones en el dispositivo con el servicio web de MDM para iOS instalado:

1. Agregue las siguientes cadenas al registro:

   - Para sistemas operativos de 32 bits:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<Nombre de host del proxy>"
"ApnProxyPort"="<Puerto del proxy>"
"ApnProxyLogin"="<Nombre de usuario para el proxy>"
"ApnProxyPwd"="<Contraseña para el proxy>"
```

   - Para sistemas operativos de 64 bits:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<Nombre de host del proxy>"
"ApnProxyPort"="<Puerto del proxy>"
"ApnProxyLogin"="<Nombre de usuario para el proxy>"
"ApnProxyPwd"="<Contraseña para el proxy>"
```

2. Reinicie el servicio web de MDM para iOS.

### Emisión e instalación de un certificado compartido en un dispositivo móvil

*Para entregar un certificado compartido a un usuario:*

1. En el árbol de consola, en la carpeta **Cuentas de usuario**, seleccione una cuenta de usuario.
2. En el menú contextual de la cuenta de usuario, seleccione **Instalar certificado**.

   Se inicia el Asistente de instalación de certificados. Siga las instrucciones del asistente.

Cuando el Asistente finaliza, se creará un certificado y este se agregará a la lista de los certificados del usuario.

El usuario descargará el certificado emitido, junto con el paquete de instalación que contiene el perfil de MDM para iOS.

Luego de que el dispositivo móvil se conecte al Servidor de MDM para iOS, se aplicará la configuración del perfil de MDM para iOS en el dispositivo del usuario. El administrador podrá administrar el dispositivo una vez que se realice la conexión.

El dispositivo móvil del usuario conectado al Servidor de MDM para iOS se muestra en la subcarpeta **Dispositivos móviles** que se encuentra en la carpeta **Administración de dispositivos móviles** en el árbol de consola.

## Incorporación de un dispositivo KES a la lista de dispositivos administrados

*Para agregar el dispositivo KES de un usuario a la lista de dispositivos administrados usando un enlace a Google Play™:*

1. En el árbol de consola, seleccione la carpeta **Cuentas de usuario**.

   De manera predeterminada, la carpeta **Cuentas de usuario** es una subcarpeta de la carpeta **Avanzado**.
2. Seleccione la cuenta de usuario a la que pertenece el dispositivo móvil que quiere agregar a la lista de dispositivos administrados.
3. En el menú contextual de la cuenta de usuario, seleccione **Agregar dispositivo móvil**.

   El Asistente para conectar un nuevo dispositivo móvil empieza a ejecutarse. En la ventana **Origen del certificado** del Asistente, indique el método de creación del certificado compartido, con el que el Servidor de administración identificará el dispositivo móvil. Puede especificar un certificado compartido usando uno de los siguientes métodos:

   - Crear un certificado compartido automáticamente (con las herramientas del Servidor de administración) y luego entregarlo al dispositivo.
   - Especificar el archivo de un certificado compartido.
4. En la ventana **Tipo de dispositivo** del Asistente, seleccione **Vínculo a Google Play**.
5. En la ventana **Método de notificación al usuario** del Asistente, indique cómo se le notificará al usuario del dispositivo móvil que el certificado se ha creado (a través de un mensaje de texto, por correo electrónico o mediante la visualización de información cuando el Asistente finalice).
6. En la ventana Información del certificado del Asistente, haga clic en el botón **Finalizar** para cerrar el Asistente.

Una vez que el Asistente finalice sus actividades, el usuario recibe en el dispositivo móvil un vínculo y un código QR para descargar Kaspersky Endpoint Security de Google Play. El usuario escanea el código QR o utiliza el enlace para ir a Google Play. A continuación, el sistema operativo del dispositivo le solicita que acepte la instalación de Kaspersky Endpoint Security para Android. Al concluir la descarga e instalación de Kaspersky Endpoint Security para Android, el dispositivo móvil se conecta con el Servidor de administración y descarga un certificado compartido. Una vez que el certificado se instala en el dispositivo móvil, el dispositivo aparece en la carpeta **Dispositivos móviles**, que es una subcarpeta de la carpeta **Administración de dispositivos móviles** en el árbol de consola.

Si Kaspersky Endpoint Security para Android ya se ha instalado en el dispositivo, el usuario tiene que recibir la configuración de conexión del Servidor de administración del administrador e ingresarla por su cuenta. Una vez definida la configuración de conexión, el dispositivo móvil se conecta al Servidor de administración. El administrador emite un certificado compartido para el dispositivo y envía al usuario un mensaje de correo electrónico o un SMS con un nombre de usuario y una contraseña para la descarga del certificado. El usuario descarga e instala el certificado compartido. Una vez que el certificado se instala en el dispositivo móvil, el dispositivo aparece en la carpeta **Dispositivos móviles**, que es una subcarpeta de la carpeta **Administración de dispositivos móviles** en el árbol de consola. En tal caso, se omitirá el paso de descarga e instalación de Kaspersky Endpoint Security para Android.

## Conexión de dispositivos KES al Servidor de administración

Kaspersky Device Management for iOS es compatible con dos esquemas o modos de conectar los dispositivos KES al Servidor de administración:

- Esquema en el que los dispositivos se conectan en forma directa al Servidor de administración
- Esquema de despliegue que involucra un proxy inverso compatible con la delegación restringida de Kerberos

### Conexión directa de dispositivos al Servidor de administración

Los dispositivos KES pueden conectarse directamente al puerto 13292 del Servidor de administración.

Según el método usado para la autenticación, dos opciones son posibles para la conexión de dispositivos KES al Servidor de administración:

- Conectar dispositivos con un certificado cliente (certificado de usuario)
- Conectar dispositivos sin un certificado cliente (certificado de usuario)

### Conectar un dispositivo con un certificado cliente (certificado de usuario)

Al conectar un dispositivo con un certificado cliente (certificado de usuario), ese dispositivo está asociado a la cuenta de usuario a la cual el certificado correspondiente se ha asignado a través de herramientas del Servidor de administración.

En este caso, se utilizará la autenticación SSL bidireccional (autenticación mutua). Tanto el Servidor de administración como el dispositivo serán autenticados con certificados.

## Conectar un dispositivo sin un certificado cliente (certificado de usuario)

Al conectar un dispositivo sin un certificado cliente (certificado de usuario), ese dispositivo no está asociado a ninguna de las cuentas de usuario en el Servidor de administración. Pero cuando el dispositivo reciba un certificado, este dispositivo se vinculará al usuario al que el Servidor de administración le haya asignado el certificado correspondiente.

Al conectar ese dispositivo al Servidor de administración, la Autenticación SSL unidireccional se aplicará, lo que significa que solo el Servidor de administración se autentica con el certificado. Después de que el dispositivo reciba el certificado cliente (certificado de usuario), el tipo de autenticación cambiará a la autenticación SSL bidireccional (autenticación SSL de 2 modos, autenticación mutua).

## Esquema para conectar dispositivos KES al Servidor en el que se usa la delegación restringida de Kerberos (KCD)

El esquema para conectar dispositivos KES al Servidor de administración utilizando la delegación restringida de Kerberos (KCD) permite lo siguiente:

- Integración con un proxy inverso compatible con KCD.
- Uso de la delegación restringida de Kerberos (denominado en lo sucesivo KCD) para la autenticación de dispositivos móviles.
- Integración con una infraestructura de claves públicas (denominada, en lo sucesivo, PKI) para aplicar certificados de usuario.

Al usar este esquema de distribución, tenga en cuenta lo siguiente:

- El tipo de conexión de dispositivos KES al proxy inverso debe ser la "autenticación SSL bidireccional", es decir, un dispositivo debe conectarse al proxy inverso a través de su certificado de usuario de propiedad. Para hacer esto, tiene que integrar el certificado cliente (certificado de usuario) en el paquete de instalación de Kaspersky Endpoint Security para Android, que se ha instalado en el dispositivo. Este paquete KES debe ser creado por el Servidor de administración expresamente para este dispositivo (usuario).

- Debe especificar el certificado (personalizado) especial en vez del certificado del servidor predeterminado para el protocolo móvil:

  1. En la ventana de Propiedades del Servidor de administración, en la sección **Configuración**, seleccione la casilla **Abrir puerto para dispositivos móviles** y seleccione **Agregar certificado** en la lista desplegable.

  2. En la ventana que se abre, especifique el mismo certificado que se configuró en el proxy inverso cuando el punto de acceso al protocolo móvil se publicó en el Servidor de administración.

- Los certificados de usuario para dispositivos KES deben ser emitidos por la Entidad de certificación (CA) del dominio. Tenga en cuenta que si el dominio incluye varias CA originales, los certificados de usuario deben ser emitidos por la CA que se haya configurado en la publicación del proxy inverso.

  Se puede asegurar de que el certificado cliente (certificado de usuario) cumpla con el requisito descrito anteriormente usando uno de los métodos siguientes:

  - Especifique el certificado de usuario especial en el Asistente de nuevo paquete y en el Asistente de instalación de certificados.

  - Integre el Servidor de administración con PKI del dominio y defina el parámetro correspondiente en las reglas para la emisión de certificados:

    1. En el árbol de consola, expanda la carpeta **Administración de dispositivos móviles** y seleccione la subcarpeta **Certificados**.

    2. En el espacio de trabajo de la carpeta **Certificados**, haga clic en el botón **Configurar reglas de emisión de certificados** para abrir la ventana **Reglas de emisión de certificados**.

    3. En la sección **Integración con PKI**, configure la integración con la Infraestructura de clave pública.

    4. En la sección **Emisión de certificados para dispositivos móviles**, especifique el origen de los certificados.

A continuación se muestra un ejemplo de instalación de la delegación restringida de Kerberos (KCD) con las siguientes suposiciones:

- El punto del acceso al protocolo móvil en el Servidor de administración está configurado en el puerto 13292.

- El nombre del dispositivo con el proxy inverso es firewall.mydom.local.

- El nombre del dispositivo con el Servidor de administración es ksc.mydom.local.

- El Nombre de la publicación externa del punto de acceso al protocolo móvil es kes4mob.mydom.global.

## Cuenta del dominio para el Servidor de administración

Debe crear una cuenta de dominio (por ejemplo, KSCMobileSrvcUsr) bajo la cual se ejecutará el servicio del Servidor de administración. Puede especificar una cuenta para el servicio del Servidor de administración al instalar el Servidor de administración o a través de la utilidad klsrvswch. La utilidad klsrvswch se localiza en la carpeta de instalación del Servidor de administración. La ruta de instalación predeterminada: <Disk>:\Archivos de programa (x86)\Kaspersky Lab\Kaspersky Security Center.

Una cuenta de dominio debe ser especificada por las siguientes razones:

- La función para la administración de dispositivos KES es una parte integral del Servidor de administración.
- Para asegurar un correcto funcionamiento de la delegación restringida de Kerberos (KCD), el lado de recepción (por ej., el Servidor de administración) se debe ejecutar bajo una cuenta de dominio.

## Nombre principal del servicio para http/kes4mob.mydom.local

En el dominio, bajo la cuenta KSCMobileSrvcUsr, agregue un SPN para publicar el servicio del protocolo móvil en el puerto 13292 del dispositivo con el Servidor de administración. Para el dispositivo kes4mob.mydom.local con el Servidor de administración, esto aparecerá de la forma siguiente:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

## Configuración de las propiedades del dominio del dispositivo con el proxy inverso (firewall.mydom.local)

Para delegar el tráfico, delegue el dispositivo con el proxy inverso (firewall.mydom.local) al servicio que es definido por SPN (http/iosmdm.mydom.local).

*Para delegar el dispositivo con el proxy inverso al servicio definido por SPN (http/iosmdm.mydom.local), el administrador debe realizar las siguientes acciones:*

1. En el complemento de Microsoft Management Console denominado "Usuarios y equipos de Active Directory", seleccione el dispositivo con el proxy inverso instalado (firewall.mydom.local).
2. En las propiedades del dispositivo, en la pestaña **Delegación**, configure la opción **Confiar este equipo para delegación para un servicio especificado únicamente** en **Usar cualquier protocolo de autenticación**.
3. En los **Servicios en los cuales esta cuenta puede presentar credenciales delegada**, agregue SPN http/kes4mob.mydom.local:13292.

## Certificado especial (personalizado) para la publicación (kes4mob.mydom.global)

Para publicar el protocolo móvil del Servidor de administración, debe emitir un certificado (personalizado) especial para FQDN kes4mob.mydom.global y especificarlo en vez del certificado del servidor predeterminado en la configuración del protocolo móvil del Servidor de administración en la Consola de administración. Para hacerlo, en la ventana de propiedades del Servidor de administración, en la sección **Configuración**, seleccione la casilla **Abrir puerto para dispositivos móviles** y luego seleccione **Agregar certificado** en la lista desplegable.

Tenga en cuenta que el contenedor del certificado del servidor (el archivo con la extensión p12 o pfx) también debe contener una cadena de certificados raíz (claves públicas).

## Configuración de la publicación en el proxy inverso

En el proxy inverso, para el tráfico que va desde un dispositivo móvil al puerto 13292 de kes4mob.mydom.global, tiene que configurar KCD en SPN (http/kes4mob.mydom.local:13292) usando el certificado del servidor emitido para FQND (kes4mob.mydom.global). Tenga en cuenta que la publicación y el punto de acceso publicado (puerto 13292 del Servidor de administración) deben compartir el mismo certificado del servidor.

## Usar Firebase Cloud Messaging

Para asegurar la distribución a tiempo de los comandos a los dispositivos KES administrados por el sistema operativo Android, Kaspersky Security Center utiliza el mecanismo de notificaciones push. Las notificaciones push se intercambian entre los dispositivos KES y el Servidor de administración a través de Firebase Cloud Messaging (en adelante, FCM). En la Consola de administración de Kaspersky Security Center, puede especificar la configuración de Firebase Cloud Messaging para conectar los dispositivos KES al servicio.

Para recuperar la configuración de Firebase Cloud Messaging, debe tener una cuenta de Google.

*Para habilitar el uso de FCM:*

1. En la Consola de administración, seleccione el nodo **Administración de dispositivos móviles** y la carpeta **Dispositivos móviles**.
2. En el menú contextual de la carpeta **Dispositivos móviles**, seleccione **Propiedades**.
3. En las propiedades de la carpeta, seleccione la sección **Configuración de Firebase Cloud Messaging**.
4. En el campo **Número de proyecto de Firebase**, especifique el Id. del remitente de FCM.
5. En el campo **Archivo de clave privada (en formato JSON)**, seleccione el archivo de clave privada.

   En la próxima sincronización con el Servidor de administración, los dispositivos KES administrados por sistemas operativos Android estarán conectados a Firebase Cloud Messaging.

Puede editar la configuración de Firebase Cloud Messaging al hacer clic en el botón **Restablecer configuración**.

Cuando cambia a otro proyecto de Firebase, debe esperar 10 minutos para que FCM reanude su ejecución.

El servicio de FCM opera en los siguientes intervalos de direcciones:

- Desde el lado del dispositivo KES, el acceso se requiere para los puertos 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) y 5230 (HTTPS) de las direcciones siguientes:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Todas las direcciones IP incluidas en el ASN 15169, perteneciente a Google
- Del lado del Servidor de administración, se requiere acceso al puerto 443 (HTTPS) de las siguientes direcciones:
  - fcm.googleapis.com
  - Todas las direcciones IP incluidas en el ASN 15169, perteneciente a Google

Si la configuración del servidor proxy (**Avanzado**/**Configuración de acceso a Internet**) se ha especificado en las propiedades del Servidor de administración en la Consola de administración, se utilizarán para la interacción con FCM.

## Configuración de FCM: obtener el Id. del remitente y el archivo de clave privada

*Para configurar FCM:*

1. Regístrese en el portal de Google.
2. Vaya a la consola de Firebase.
3. Realice una de las siguientes acciones:
   - Para crear un nuevo proyecto, haga clic en **Crear un proyecto** y siga las instrucciones en pantalla.
   - Abra un proyecto existente.
4. Haga clic en el ícono de ajustes y seleccione **Configuración del proyecto**.
   Se abre la ventana **Configuración del proyecto**.
5. Seleccione la pestaña **Cloud Messaging**.
6. Recupere el id. del remitente correspondiente del campo **Id. del remitente** en la sección **API de Firebase Cloud Messaging (V1)**.
7. Seleccione la pestaña **Cuentas de servicio** y haga clic en **Generar nueva clave privada**.
8. En la ventana que se abre, haga clic en **Generar clave** para generar y descargar un archivo de clave privada.

Firebase Cloud Messaging queda configurado.

# Integración con una infraestructura de claves públicas

La integración con la infraestructura de claves públicas (denominada en lo sucesivo PKI) se creó principalmente para simplificar la emisión de certificados de usuario del dominio por el Servidor de administración.

El administrador puede asignar un certificado de dominio para un usuario en la Consola de administración. Esto se puede hacer usando uno de los siguientes métodos:

- Asigne al usuario un certificado especial (personalizado) desde un archivo en el Asistente de instalación de certificados.
- Realice la integración con PKI y asigne PKI para que actúe como origen de certificados para un tipo concreto de certificados o para todos los tipos de certificados.

La configuración de integración con PKI está disponible en el espacio de trabajo de la carpeta **Administración de dispositivos móviles** / / **Certificados** al hacer clic en el enlace **Integrar con infraestructura de claves públicas**.

## Principio general de integración con PKI para emisión de certificados de usuario del dominio

En la Consola de administración, haga clic en el enlace **Integrar con infraestructura de claves públicas** en el espacio de trabajo de la carpeta **Administración de dispositivos móviles** / **Certificados** para especificar una cuenta de dominio que utilizará el Servidor de administración para emitir certificados de usuario del dominio a través de las CA del dominio (denominado en lo sucesivo la cuenta mediante la cual se realiza la integración con PKI).

Tenga en cuenta lo siguiente:

- La configuración de integración con PKI le proporciona la posibilidad de especificar la plantilla predeterminada para todos los tipos de certificados. Tenga en cuenta que las reglas para la emisión de certificados (disponibles en el espacio de trabajo de la carpeta **Administración de dispositivos móviles** / **Certificados**, al hacer clic en el botón **Configurar reglas de emisión de certificados**), le permiten especificar una plantilla individual para cada tipo de certificados.
- Un certificado especial del Agente de inscripción (EA) se debe instalar en el dispositivo con el Servidor de administración, en el repositorio de certificados de la cuenta bajo la cual la integración con PKI se realiza. El certificado del Agente de inscripción (EA) es emitido por el administrador del CA del dominio (Entidad de certificación).

La cuenta bajo la cual la integración con PKI se realiza debe cumplir los criterios siguientes:

- Es un usuario de dominio.
- Es un administrador local del dispositivo con el Servidor de administración desde el cual la integración con PKI se inicia.
- Tiene derecho a *Iniciar sesión como servicio*.
- El dispositivo con el Servidor de administración instalado se debe ejecutar al menos una vez bajo esta cuenta para crear un perfil de usuario permanente.

## Servidor web de Kaspersky Security Center

Servidor web de Kaspersky Security Center (denominado en lo sucesivo Servidor web) es un componente de Kaspersky Security Center. El Servidor web está diseñado para publicar paquetes de instalación independientes, paquetes de instalación independientes para dispositivos móviles, perfiles de MDM para iOS y archivos de la carpeta compartida.

Los perfiles de MDM para iOS y los paquetes de instalación que se han creado se publican en el Servidor web automáticamente y luego se eliminan después de la primera descarga. El administrador puede enviar el nuevo enlace al usuario de cualquier manera que le resulte conveniente (por ejemplo, por correo electrónico).

Al hacer clic en este enlace, el usuario puede descargar la información solicitada a un dispositivo móvil.

### Configuración del Servidor web

Si se requiere poner a punto el Servidor web, las propiedades del Servidor web de la Consola de administración proporcionan la posibilidad de cambiar puertos para HTTP (8060) y HTTPS (8061). Además del cambio de puertos, puede reemplazar el certificado del servidor para HTTPS y cambiar FQDN del Servidor web para HTTP.

# Instalación de Kaspersky Security Center

Esta sección describe la instalación de los componentes de Kaspersky Security Center. Si desea instalar la aplicación de manera local en un solo dispositivo, hay dos opciones de instalación disponibles:

- **Estándar**. Se recomienda esta opción si desea probar Kaspersky Security Center, por ejemplo, al probar su funcionamiento en un área pequeña dentro su red. Durante la instalación estándar, solo se configura la base de datos. También puede instalar solo el conjunto predeterminado de complementos de administración para las aplicaciones de Kaspersky. También puede utilizar la instalación estándar si ya tiene experiencia de trabajo con Kaspersky Security Center y sabe cómo especificar todas las configuraciones relevantes después de la instalación estándar.

- **Personalizada**. Se recomienda esta opción si planea modificar la configuración de Kaspersky Security Center, como la ruta a la carpeta compartida, las cuentas y los puertos para la conexión con el Servidor de administración y la configuración de la base de datos. La instalación personalizada le permite especificar qué complementos de administración de Kaspersky instalar. Si es necesario, puede iniciar la instalación personalizada en el modo no interactivo.

Si al menos un Servidor de administración se instala en la red, los Servidores se pueden instalar en otros dispositivos remotamente a través de la tarea de instalación remota usando la instalación forzada. Para crear la tarea de instalación remota, utilice el paquete de instalación del Servidor de administración llamado “ksc_<número de versión>.<número de compilación>_full_<idioma de localización>.exe”.

Use este paquete si desea instalar todos los componentes requeridos para la funcionalidad completa de Kaspersky Security Center o actualizar las versiones actuales de estos componentes.

Si desea implementar el clúster de conmutación por error de Kaspersky Security Center, debe instalar Kaspersky Security Center en todos los nodos del clúster.

# Preparación para la instalación

Realice las siguientes acciones antes de iniciar la instalación.

- **Verifique los requisitos de hardware y software**

  Asegúrese de que el hardware y el software del dispositivo cumplan los requisitos del Servidor de administración y la Consola de administración.

- **Seleccione e instale el sistema de gestión de bases de datos (DBMS)**

  Kaspersky Security Center almacena su información en una base de datos administrada por un DBMS. Instale el DBMS en la red antes de instalar Kaspersky Security Center (más información sobre cómo seleccionar un DBMS). Si decide instalar PostgreSQL o Postgres Pro DBMS, especifique una contraseña para el superusuario. Si no especifica esta contraseña, es posible que el Servidor de administración no pueda conectarse a la base de datos.

  Se recomienda instalar el Servidor de administración en un servidor dedicado y no en un controlador de dominio. Sin embargo, si instala Kaspersky Security Center en un servidor que actúe como controlador de dominio de solo lectura (RODC), Microsoft SQL Server (SQL Express) no se debe instalar de manera local (en el mismo dispositivo). En este caso, le recomendamos que instale Microsoft SQL Server (SQL Express) de forma remota (en un dispositivo diferente) o que use MySQL, MariaDB o PostgreSQL si necesita instalar el DBMS de manera local.

- **Preparar carpetas para el Servidor de administración, el Agente de red y la Consola de administración**

  El Servidor de administración, el Agente de red y la Consola de administración deben instalarse en carpetas que tengan deshabilitada la distinción entre mayúsculas y minúsculas. Además, la distinción entre mayúsculas y minúsculas debe estar deshabilitada para la carpeta compartida del Servidor de administración y la carpeta oculta de Kaspersky Security Center (%ALLUSERSPROFILE%\KasperskyLab\adminkit).

- **Eliminar el Agente de red anterior**

  La versión de servidor del Agente de red se instala en el dispositivo junto con el Servidor de administración. El Servidor de administración no puede instalarse junto con la versión regular del Agente de red. Si la versión de servidor del Agente de red ya se encuentra instalada en el dispositivo, elimínela y reinicie la instalación del Servidor de administración. Para obtener detalles sobre la versión del servidor del Agente de red, consulte Cambios en el sistema después de la instalación de Kaspersky Security Center.

- **Comprobar cuentas**

  La instalación de Kaspersky Security Center requiere derechos del administrador en el dispositivo en el cual se realizará la instalación.

  Kaspersky Security Center admite cuentas de servicio administradas y cuentas de servicio administradas por grupos. Si estos tipos de cuentas se utilizan en su dominio y usted desea especificar una de ellas como la cuenta para el servicio del Servidor de administración, primero instale la cuenta en el mismo dispositivo en el que desea instalar el Servidor de administración. Para obtener más información sobre la instalación de cuentas de servicio administradas en un dispositivo local, consulte la documentación oficial de Microsoft.

# Cuentas para trabajar con el DBMS

Para instalar el Servidor de administración y trabajar con él, necesita una cuenta de Windows con la que ejecutará el instalador del Servidor de administración (en adelante, también denominado instalador), una cuenta de Windows con la que iniciará el servicio del Servidor de administración y una cuenta de DBMS interna para acceder al DBMS. Puede crear cuentas nuevas o utilizar cuentas existentes. Cada cuenta debe tener derechos específicos. El conjunto de cuentas necesarias y sus derechos depende de los siguientes criterios:

- Tipo de DBMS:
  - Microsoft SQL Server (con autenticación de Windows o autenticación de SQL Server)
  - MySQL o MariaDB
  - PostgreSQL o Postgres Pro
- Ubicación del DBMS:
  - **DBMS local**. Un *DBMS local* es un DBMS instalado en el mismo dispositivo que el Servidor de administración.
  - **DBMS remoto**. Un *DBMS remoto* es un DBMS instalado en un dispositivo diferente.
- Método de creación de la base de datos del Servidor de administración:
  - **Automático**. Durante la instalación del Servidor de administración, puede crear automáticamente una base de datos del Servidor de administración (en adelante, también denominada como una base de datos del Servidor) usando el instalador.
  - **Manual**. Puede crear una base de datos vacía utilizando un script o una aplicación de un tercero (por ejemplo, SQL Server Management Studio). Luego, durante la instalación del Servidor de administración, puede usar esa base de datos vacía como base de datos para el Servidor de administración.

A la hora de asignar derechos y permisos a las cuentas, limítese a lo justo y necesario. Dicho de otro modo, no asigne más derechos que los que se necesiten para llevar a cabo las acciones necesarias.

En las siguientes tablas, encontrará información sobre los derechos del sistema y los derechos de DBMS que deberá otorgar a las cuentas antes de instalar e iniciar el Servidor de administración.

## Microsoft SQL Server con autenticación de Windows

Si elige SQL Server como DBMS, puede usar la autenticación de Windows para acceder a SQL Server. Configure los derechos del sistema para una cuenta de Windows utilizada para ejecutar el instalador y de una cuenta de Windows utilizada para iniciar el servicio del Servidor de administración. En SQL Server, cree credenciales de inicio de sesión para ambas cuentas de Windows. En la siguiente tabla, se detallan los derechos de SQL Server necesarios que deberá asignar a estas cuentas según el método elegido para crear la base de datos del Servidor. Para obtener más información sobre cómo configurar los derechos del rol, consulte Configuración de cuentas para trabajar con SQL Server (autenticación de Windows).

DBMS: Microsoft SQL Server (puede ser Express Edition) con autenticación de Windows

| | Base de datos creada automáticamente (por el instalador) | Base de datos creada manualmente (por el administrador) |
|---|---|---|
| **Cuenta con la cual se está ejecutando el instalador** | • DBMS remoto: solo una cuenta de dominio del dispositivo remoto en el que esté instalado el DBMS.<br>• DBMS local: una cuenta de administrador local o una cuenta de dominio. | • DBMS remoto: solo una cuenta de dominio del dispositivo remoto en el que esté instalado el DBMS.<br>• DBMS local: una cuenta de administrador local o una cuenta de dominio. |
| **Derechos de la cuenta con la cual se está ejecutando el instalador** | • Derechos del sistema: derechos de administrador local.<br>• Derechos del servidor SQL:<br>  • Rol de nivel servidor: sysadmin. | • Derechos del sistema: derechos de administrador local.<br>• Derechos del servidor SQL:<br>  • Rol de nivel servidor: public.<br>  • Membrecía en roles de bases de datos para la base de datos del Servidor: db_owner, public.<br>  • Esquema predeterminado para la base de datos del Servidor: dbo. |
| **Cuenta del servicio del Servidor de administración** | • DBMS remoto: solo una cuenta de dominio del dispositivo remoto en el que esté instalado el DBMS.<br>• DBMS local:<br>  • Una cuenta de Windows elegida por el administrador.<br>  • Una cuenta en formato KL-AK-*, creada automáticamente por el instalador. | • DBMS remoto: solo una cuenta de dominio del dispositivo remoto en el que esté instalado el DBMS.<br>• DBMS local:<br>  • Una cuenta de Windows elegida por el administrador.<br>  • Una cuenta en el formato KL-AK-* que el instalador crea automáticamente (en este caso, no recomendamos generar una cuenta KL-AK-*). |
| **Derechos de la cuenta del servicio del Servidor de administración** | • Derechos del sistema: los derechos necesarios son asignados por el instalador.<br>• Derechos de SQL Server: los derechos necesarios son asignados por el instalador. | • Derechos del sistema: los derechos necesarios son asignados por el instalador.<br>• Derechos de SQL Server:<br>  • Rol de nivel servidor: public.<br>  • Membrecía en roles de bases de datos para la base de datos del Servidor: db_owner, public.<br>  • Esquema predeterminado para la base de datos del Servidor: dbo. |

## Microsoft SQL Server con autenticación de SQL Server

Si elige SQL Server como DBMS, puede usar la autenticación de SQL Server para acceder a SQL Server. Configure los derechos del sistema para una cuenta de Windows utilizada para ejecutar el instalador y para una cuenta de Windows utilizada para iniciar el servicio del Servidor de administración. En SQL Server, cree el usuario con contraseña que se usará para la autenticación. Luego, otorgue a esta nueva cuenta de SQL Server los derechos necesarios (detallados en la siguiente tabla). Para más información sobre cómo configurar los derechos del rol, consulte Configuración de cuentas para trabajar con SQL Server (autenticación de SQL Server).

DBMS: Microsoft SQL Server (puede ser Express Edition) con autenticación de SQL Server

| | Base de datos creada automáticamente (por el instalador) | Base de datos creada manualmente (por el administrador) |
|---|---|---|
| **Cuenta con la cual se está ejecutando el instalador** | • DBMS remoto: solo una cuenta de dominio del dispositivo remoto en el que esté instalado el DBMS.<br>• DBMS local: una cuenta de administrador local o una cuenta de dominio. | • DBMS remoto: solo una cuenta de dominio del dispositivo remoto en el que esté instalado el DBMS.<br>• DBMS local: una cuenta de administrador local o una cuenta de dominio. |
| **Derechos de la cuenta con la cual se está ejecutando el instalador** | Derechos del sistema: derechos de administrador local. | Derechos del sistema: derechos de administrador local. |

| | Base de datos creada automáticamente (por el instalador) | Base de datos creada manualmente (por el administrador) |
|---|---|---|
| **Cuenta del servicio del Servidor de administración** | • DBMS remoto: solo una cuenta de dominio del dispositivo remoto en el que esté instalado el DBMS.<br>• DBMS local:<br>  • Una cuenta de Windows elegida por el administrador.<br>  • Una cuenta en formato KL-AK-*, creada automáticamente por el instalador. | • DBMS remoto: solo una cuenta de dominio del dispositivo remoto en el que esté instalado el DBMS.<br>• DBMS local:<br>  • Una cuenta de usuario de Windows elegida por el administrador.<br>  • Una cuenta en formato KL-AK-*, creada automáticamente por el instalador. |
| **Derechos de la cuenta del servicio del Servidor de administración** | Derechos del sistema: los derechos necesarios son asignados por el instalador. | Derechos del sistema: los derechos necesarios son asignados por el instalador. |
| **Derechos del usuario utilizado para autenticarse en SQL Server** | Derechos de SQL Server que se necesitan para crear una base de datos e instalar el Servidor de administración:<br>• Rol de nivel servidor: public.<br>• Pertenencia del rol de base de datos para la base de datos *maestra*: db_owner.<br>• Esquema predeterminado para la base de datos *maestra*: dbo.<br>• Permisos:<br>  • CONNECT ANY DATABASE<br>  • CONNECT SQL<br>  • CREATE ANY DATABASE<br>  • VIEW ANY DATABASE<br>  • VIEW SERVER STATE (si la opción **Always On** está habilitada)<br>Derechos de SQL Server que se necesitan para operar con el Servidor de administración:<br>• Rol de nivel servidor: public.<br>• Membrecía en roles de bases de datos para la base de datos del Servidor: db_owner.<br>• Esquema predeterminado para la base de datos del Servidor: dbo.<br>• Permisos:<br>  • CONNECT SQL<br>  • VIEW ANY DATABASE<br>  • VIEW SERVER STATE (si la opción **Always On** está habilitada)<br>  • VER CUALQUIER DEFINICIÓN | Derechos de SQL Server:<br>• Rol de nivel servidor: public.<br>• Membrecía en roles de bases de datos para la base de datos del Servidor: db_owner.<br>• Esquema predeterminado para la base de datos del Servidor: dbo.<br>• Permisos:<br>  • CONNECT SQL<br>  • VIEW ANY DATABASE<br>  • VER CUALQUIER DEFINICIÓN |

## Configuración de los derechos de SQL Server para recuperar los datos del Servidor de administración

Para restaurar los datos del Servidor de administración desde la copia de seguridad, ejecute la utilidad klbackup con la cuenta de Windows utilizada para instalar el Servidor de administración. Antes de iniciar la utilidad klbackup, en SQL Server, otorgue los derechos necesarios al usuario de SQL Server asociado con esa cuenta de Windows. Los derechos de SQL Server varían según la versión del Servidor de administración. Para el Servidor de administración de la versión 14.2 o posterior, puede otorgar la función de nivel de servidor sysadmin o la función de nivel de servidor dbcreator.

Derechos de SQL Server para la recuperación de la base de datos del Servidor de administración

| Versión 14.2 o posterior del Servidor de administración | Otras versiones del Servidor de administración |
|---|---|
| • Derechos de SQL Server:<br>  • Rol de nivel servidor: dbcreator.<br>• Permisos:<br>  • VER CUALQUIER DEFINICIÓN<br>Antes de iniciar la utilidad klbackup, especifique el indicador de servidor KLSRV_SKIP_ADJUSTING_DBMS_ACCESS. Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada es <Disk>:\Archivos de programa(x86)\Kaspersky Lab\Kaspersky Security Center. Luego, ejecute el siguiente comando en la línea de comandos:<br>`klscflag.exe -fset -pv klserver -n KLSRV_SKIP_ADJUSTING_DBMS_ACCESS -t d -v 1` | |

## MySQL y MariaDB

Si elige MySQL o MariaDB como DBMS, cree una cuenta interna en el DBMS y otorgue a esa cuenta los derechos necesarios (detallados en la siguiente tabla). El instalador y el servicio del Servidor de administración usarán esta cuenta interna del DBMS para acceder al DBMS. Tenga presente que el conjunto de derechos necesarios es siempre el mismo, independientemente del método utilizado para crear la base de datos. Para más información sobre cómo configurar los derechos de la cuenta, consulte Configuración de cuentas para trabajar con MySQL y MariaDB.

DBMS: MySQL y MariaDB

| | Base de datos creada manual o automáticamente |
|---|---|
| **Cuenta con la cual se está ejecutando el instalador** | • DBMS remoto: solo una cuenta de dominio del dispositivo remoto en el que esté instalado el DBMS.<br>• DBMS local: una cuenta de administrador local o una cuenta de dominio. |
| **Derechos de la cuenta con la cual se está ejecutando el instalador** | Derechos del sistema: derechos de administrador local. |
| **Cuenta del servicio del Servidor de administración** | • DBMS remoto: solo una cuenta de dominio del dispositivo remoto en el que esté instalado el DBMS.<br>• DBMS local:<br>  • Una cuenta de Windows elegida por el administrador.<br>  • Una cuenta en formato KL-AK-*, creada automáticamente por el instalador. |
| **Derechos de la cuenta del servicio del Servidor de administración** | Derechos del sistema: los derechos necesarios son asignados por el instalador. |
| **Derechos de la cuenta interna del DBMS** | Privilegios de esquema:<br>• Base de datos del Servidor de administración: ALL (excepto GRANT OPTION).<br>• Esquemas del sistema (mysql y sys): SELECT, SHOW VIEW.<br>• Procedimiento almacenado "sys.table_exists": EXECUTE (si su DBMS es MariaDB versión 10.5 o anterior, no necesita otorgar el privilegio EXECUTE).<br>Privilegios globales para todos los esquemas: PROCESS, SUPER. |

Para obtener detalles sobre cómo mover datos de un espacio de tabla compartido a un espacio de tabla por archivo, consulte Mover datos de un espacio de tabla compartido a un espacio de tabla por archivo en los DBMS MySQL y MariaDB.

## Configuración de privilegios para recuperar los datos del Servidor de administración

Los derechos asignados a la cuenta interna del DBMS bastan para restaurar los datos del Servidor de administración utilizando una copia de seguridad. Para iniciar la restauración, ejecute la utilidad klbackup con la cuenta de Windows que se haya utilizado para instalar el Servidor de administración.

## PostgreSQL o Postgres Pro

Si elige PostgreSQL o Postgres Pro como DBMS, puede usar el usuario *Postgres* (el rol predeterminado de Postgres) o puede crear un nuevo rol de Postgres (en lo sucesivo, también denominado rol) para acceder al DBMS. En la siguiente tabla, se detallan los derechos que deberá asignar a este rol según el método elegido para crear la base de datos del Servidor. Para más información sobre cómo configurar los derechos del rol, consulte Configuración de cuentas para trabajar con PostgreSQL o Postgres Pro.

DBMS: PostgreSQL o Postgres Pro

| | Base de datos creada automáticamente | | Base de datos creada manualmente |
|---|---|---|---|
| **Cuenta con la cual se está ejecutando el instalador** | • DBMS remoto: solo una cuenta de dominio del dispositivo remoto en el que esté instalado el DBMS.<br>• DBMS local: una cuenta de administrador local o una cuenta de dominio. | | • DBMS remoto: solo una cuenta de dominio del dispositivo remoto con el DBMS instalado.<br>• DBMS local: una cuenta de administrador local o una cuenta de dominio. |
| **Derechos de la cuenta con la cual se está ejecutando el instalador** | Derechos del sistema: derechos de administrador local. | | Derechos del sistema: derechos de administrador local. |
| **Cuenta del servicio del Servidor de administración** | • DBMS remoto: solo una cuenta de dominio del dispositivo remoto en el que esté instalado el DBMS.<br>• DBMS local:<br>  • Una cuenta de Windows elegida por el administrador.<br>  • Una cuenta en formato KL-AK-*, creada automáticamente por el instalador. | | • DBMS remoto: solo una cuenta de dominio del dispositivo remoto con el DBMS instalado.<br>• DBMS local:<br>  • Una cuenta de Windows elegida por el administrador.<br>  • Una cuenta en formato KL-AK-*, creada automáticamente por el instalador. |
| **Derechos de la cuenta del servicio del Servidor de administración** | Derechos del sistema: los derechos necesarios son asignados por el instalador. | | Derechos del sistema: los derechos necesarios son asignados por el instalador. |
| **Derechos del rol de Postgres** | Si utiliza el usuario *Postgres*, no necesita asignar privilegios adicionales. | Privilegios para un nuevo rol: `CREATEDB`. | Si crea un nuevo rol:<br>• Privilegios en la base de datos del Servidor de administración: `ALL`.<br>• Privilegios en todas las tablas del esquema público: `ALL`.<br>• Privilegios en todas las secuencias en el esquema público: `ALL`. |

## Configuración de privilegios para recuperar los datos del Servidor de administración

Para restaurar los datos del Servidor de administración desde la copia de seguridad, ejecute la utilidad klbackup con la cuenta de Windows utilizada para instalar el Servidor de administración. Tenga en cuenta que el rol de Postgres utilizado para acceder al DBMS debe tener derechos de propietario en la base de datos del Servidor de administración.

# Configurar las cuentas para trabajar con SQL Server (autenticación de Windows)

## Requisitos previos

Antes de asignar derechos a las cuentas, realice las siguientes acciones:

1. Inicie sesión en el sistema con la cuenta del administrador local.
2. Instale un entorno para trabajar con SQL Server.
3. Asegúrese de tener una cuenta de Windows que pueda usarse para instalar el Servidor de administración.
4. Asegúrese de tener una cuenta de Windows que pueda usarse para iniciar el servicio del Servidor de administración.
5. En SQL Server, cree un inicio de sesión para la cuenta de Windows utilizada para ejecutar el instalador del Servidor de administración (en adelante, también denominado instalador). Cree, asimismo, un usuario para la cuenta de Windows utilizada para iniciar el servicio del Servidor de administración.

Si usa SQL Server Management Studio, en la página **General** de la ventana de propiedades de inicio de sesión, seleccione la opción **Autenticación de Windows**.

Si desea instalar el Servidor de administración y SQL Server en dispositivos que se encuentren en dominios de Windows separados, tenga presente que los dominios deberán tener relaciones de confianza bidireccionales para garantizar el correcto funcionamiento del Servidor de administración, incluidas la ejecución de tareas y la aplicación de directivas. Para obtener información sobre las cuentas que se necesitan para utilizar diferentes DBMS y sobre los derechos que deben tener estas cuentas, consulte Cuentas para trabajar con el DBMS.

## Configuración de las cuentas para instalar el Servidor de administración (creación automática de la base de datos del Servidor de administración)

*Para configurar las cuentas para la instalación del Servidor de administración:*

1. En SQL Server, asigne la función de rol de nivel de servidor sysadmin al inicio de sesión de la cuenta de Windows utilizada para ejecutar el instalador.
2. Inicie sesión en el sistema con la cuenta de Windows que desee usar para ejecutar el instalador.
3. Ejecute el instalador del Servidor de administración.

   Se inicia el asistente de instalación del Servidor de administración. Siga las instrucciones del asistente.
4. Seleccione la opción de instalación personalizada del Servidor de administración.
5. Seleccione Microsoft SQL Server como DBMS que almacena la base de datos del Servidor de administración.

6. Seleccione el Modo de autenticación de Microsoft Windows para establecer una conexión entre el Servidor de administración y SQL Server a través de una cuenta de Windows.

7. Introduzca el nombre de la cuenta de Windows usada para iniciar el servicio del Servidor de administración.

   Puede seleccionar la cuenta de usuario de Windows para la que creó un inicio de sesión en SQL Server. Como alternativa, puede dejar que el instalador cree automáticamente una nueva cuenta de Windows con el formato KL-AK-*. Si elige esta opción, el instalador creará automáticamente un inicio de sesión de SQL Server para la nueva cuenta. En cualquiera de los dos casos, el instalador asignará los derechos del sistema y los derechos de SQL Server necesarios a la cuenta utilizada para el servicio del Servidor de administración.

Al concluir la instalación, se habrá creado la base de datos del Servidor, y la cuenta utilizada para el servicio del Servidor de administración contará con los derechos del sistema y los derechos de SQL Server necesarios. El Servidor de administración estará entonces listo para usar.

## Configuración de las cuentas para instalar el Servidor de administración (creación manual de la base de datos del Servidor de administración)

*Para configurar las cuentas para la instalación del Servidor de administración:*

1. En SQL Server, cree una base de datos vacía. El rol creado se utilizará como propietario de la base de datos del Servidor de administración (en adelante, también denominada "base de datos del Servidor").

2. Especifique, para ambos inicios de sesión de SQL Server creados para las cuentas de Windows, el rol de nivel de servidor público y, a continuación, configure la asignación a la base de datos creada:

   - Rol de nivel servidor: "public"
   - Membrecía en roles de bases de datos: db_owner, public
   - Esquema predeterminado: dbo

3. Inicie sesión en el sistema con la cuenta de Windows que desee usar para ejecutar el instalador.

4. Ejecute el instalador del Servidor de administración.

   Se inicia el asistente de instalación del Servidor de administración. Siga las instrucciones del asistente.

5. Seleccione la opción de instalación personalizada del Servidor de administración.

6. Seleccione Microsoft SQL Server como DBMS que almacena la base de datos del Servidor de administración.

7. Especifique el nombre de la base de datos creada como el nombre de la base de datos del Servidor de administración.

8. Seleccione el Modo de autenticación de Microsoft Windows para establecer una conexión entre el Servidor de administración y SQL Server a través de una cuenta de Windows.

9. Introduzca el nombre de la cuenta de Windows usada para iniciar el servicio del Servidor de administración.

   Puede seleccionar la cuenta de usuario de Windows para la que creó un inicio de sesión en SQL Server (y a la cual asignó los correspondientes derechos en un paso anterior).

No recomendamos que cree automáticamente una nueva cuenta de Windows de formato KL-AK-*. Si lo hace, el instalador creará una nueva cuenta de Windows para la cual usted no habrá creado y configurado una cuenta de SQL Server. El Servidor de administración no podrá utilizar esa cuenta para iniciar el servicio del Servidor de administración. Si necesita crear una cuenta de Windows de formato KL-AK-*, no inicie la Consola de administración después de la instalación. Haga, en cambio, lo siguiente:

1. Detenga el servicio kladminserver.
2. En SQL Server, cree un inicio de sesión de SQL Server para la cuenta de Windows KL-AK-* que se haya creado.
3. Otorgue los derechos necesarios a este nuevo inicio de sesión de SQL Server y configure la asignación a la base de datos creada:
   - Rol de nivel servidor: "public"
   - Membrecía en roles de bases de datos: db_owner, public
   - Esquema predeterminado: dbo
4. Reinicie el servicio kladminserver y ejecute la Consola de administración.

Una vez que concluya la instalación, el Servidor de administración utilizará la base de datos creada para almacenar los datos del Servidor. El Servidor de administración estará entonces listo para usar.

# Configurar las cuentas para trabajar con SQL Server (autenticación de SQL Server)

## Requisitos previos

Antes de asignar derechos a las cuentas, realice las siguientes acciones:

1. Inicie sesión en el sistema con la cuenta del administrador local.
2. Instale un entorno para trabajar con SQL Server.
3. Asegúrese de tener una cuenta de Windows que pueda usarse para instalar el Servidor de administración.
4. Asegúrese de tener una cuenta de Windows que pueda usarse para iniciar el servicio del Servidor de administración.
5. En SQL Server, habilite el modo de autenticación de SQL Server.

   Si utiliza SQL Server Management Studio, en la página **Seguridad** de la ventana de propiedades de SQL Server, seleccione la opción **modo de autenticación de SQL Server y Windows**.
6. En SQL Server, cree un inicio de sesión con contraseña. El instalador del Servidor de administración (en adelante, también denominado "el instalador") y el servicio del Servidor de administración utilizarán la cuenta interna del DBMS para acceder al DBMS.

   Si usa SQL Server Management Studio, en la página **General** de la ventana de propiedades de inicio de sesión, seleccione la opción **Autenticación de SQL Server**.

Si desea instalar el Servidor de administración y SQL Server en dispositivos que se encuentren en dominios de Windows separados, tenga presente que los dominios deberán tener relaciones de confianza bidireccionales para garantizar el correcto funcionamiento del Servidor de administración, incluidas la ejecución de tareas y la aplicación de directivas. Para obtener información sobre las cuentas que se necesitan para utilizar diferentes DBMS y sobre los derechos que deben tener estas cuentas, consulte Cuentas para trabajar con el DBMS.

## Configuración de las cuentas para instalar el Servidor de administración (creación automática de la base de datos del Servidor de administración)

*Para configurar las cuentas para la instalación del Servidor de administración:*

1. En SQL Server, asigne la cuenta de SQL Server a la case de datos *maestra* predeterminada. La base de datos *maestra* es una plantilla para la base de datos del Servidor de Administración (en adelante, también denominada base de datos del Servidor). La base de datos *maestra* se utiliza para la asignación hasta que el instalador crea una base de datos del Servidor. Otorgue los siguientes derechos y permisos a la cuenta de SQL Server:

   - Rol de nivel servidor: "public"
   - Pertenencia del rol de base de datos para la base de datos *maestra*: db_owner
   - Esquema predeterminado para la base de datos *maestra*: dbo
   - Permisos:
     - CONNECT ANY DATABASE
     - CONNECT SQL
     - CREATE ANY DATABASE
     - VIEW ANY DATABASE

2. Inicie sesión en el sistema con la cuenta de Windows que desee usar para ejecutar el instalador.

3. Ejecute el instalador.

   Se inicia el asistente de instalación del Servidor de administración. Siga las instrucciones del asistente.

4. Seleccione la opción de instalación personalizada del Servidor de administración.

5. Seleccione Microsoft SQL Server como DBMS que almacena la base de datos del Servidor de administración.

6. Especifique el nombre de la base de datos del Servidor de administración.

7. Seleccione el modo de autenticación de SQL Server para establecer una conexión entre el Servidor de administración y SQL Server a través de la cuenta de SQL Server creada. Seguidamente, introduzca las credenciales de la cuenta de SQL Server.

8. Introduzca el nombre de la cuenta de Windows usada para iniciar el servicio del Servidor de administración.

   Puede seleccionar una cuenta de usuario de Windows existente o, mediante el instalador, crear una nueva cuenta de Windows de formato KL-AK-*. En cualquiera de los dos casos, el instalador asignará los derechos del sistema necesarios a la cuenta utilizada para el servicio del Servidor de administración.

Al concluir la instalación, se habrá creado la base de datos del Servidor, y la cuenta utilizada para el servicio del Servidor de administración contará con los derechos del sistema necesarios. El Servidor de administración estará entonces listo para usar.

Puede cancelar la asignación a la base de datos *maestra*, porque el instalador creó una base de datos del servidor y configuró la asignación a esta base de datos durante la instalación del Servidor de administración.

La creación automática de la base de datos requiere más permisos que los que se requieren para operar con el Servidor de administración normalmente; puede, por ende, revocar algunos permisos. En SQL Server, seleccione la cuenta de SQL Server y luego otorgue los siguientes derechos para operar con el Servidor de administración:

- Rol de nivel servidor: "public"
- Membrecía en roles de bases de datos para la base de datos del Servidor: db_owner
- Esquema predeterminado para la base de datos del Servidor: dbo
- Permisos:
  - CONNECT SQL
  - VIEW ANY DATABASE

## Configuración de las cuentas para instalar el Servidor de administración (creación manual de la base de datos del Servidor de administración)

*Para configurar las cuentas para la instalación del Servidor de administración:*

1. En SQL Server, cree una base de datos vacía. Se la utilizará como base de datos del Servidor de administración.
2. En SQL Server, otorgue los siguientes derechos y permisos a la cuenta de SQL Server:
   - Rol de nivel servidor: public.
   - Membrecía en roles de bases de datos para la base de datos creada: db_owner
   - Esquema predeterminado para la base de datos creada: dbo
   - Permisos:
     - CONNECT SQL
     - VIEW ANY DATABASE
3. Inicie sesión en el sistema con la cuenta de Windows que desee usar para ejecutar el instalador.
4. Ejecute el instalador.

   Se inicia el asistente de instalación del Servidor de administración. Siga las instrucciones del asistente.
5. Seleccione la opción de instalación personalizada del Servidor de administración.
6. Seleccione Microsoft SQL Server como DBMS que almacena la base de datos del Servidor de administración.
7. Especifique el nombre de la base de datos creada como el nombre de la base de datos del Servidor de administración.

8. Seleccione el modo de autenticación de SQL Server para establecer una conexión entre el Servidor de administración y SQL Server a través de la cuenta de SQL Server creada. Seguidamente, introduzca las credenciales de la cuenta de SQL Server.

9. Introduzca el nombre de la cuenta de Windows usada para iniciar el servicio del Servidor de administración.

   Puede seleccionar una cuenta de usuario de Windows existente o, mediante el instalador, crear una nueva cuenta de Windows de formato KL-AK-*. En cualquiera de los dos casos, el instalador asignará los derechos del sistema necesarios a la cuenta utilizada para el servicio del Servidor de administración.

Una vez que concluya la instalación, el Servidor de administración utilizará la base de datos creada para almacenar los datos del Servidor de administración. La cuenta utilizada para el servicio del Servidor de administración contará con todos los derechos del sistema necesarios. El Servidor de administración estará entonces listo para usar.

# Configurar las cuentas para trabajar con MySQL y MariaDB

## Requisitos previos

Antes de asignar derechos a las cuentas, realice las siguientes acciones:

1. Inicie sesión en el sistema con la cuenta del administrador local.

2. Instale un entorno para trabajar con MySQL o MariaDB.

3. Asegúrese de tener una cuenta de Windows que pueda usarse para instalar el Servidor de administración.

4. Asegúrese de tener una cuenta de Windows que pueda usarse para iniciar el servicio del Servidor de administración.

## Configuración de las cuentas para instalar el Servidor de administración

*Para configurar las cuentas para la instalación del Servidor de administración:*

1. Con la cuenta de superusuario que creó al instalar el DBMS, ejecute un entorno para trabajar con MySQL o MariaDB.

2. En el DBMS, cree una cuenta interna con contraseña. El instalador del Servidor de administración (en adelante, también denominado "el instalador") y el servicio del Servidor de administración utilizarán la cuenta interna del DBMS para acceder al DBMS. Otorgue a esta cuenta los siguientes privilegios:

   - Privilegios de esquema:
     - Base de datos del Servidor de administración: ALL (excepto `GRANT OPTION`)
     - Esquemas del sistema (mysql y sys): `SELECT`, `SHOW VIEW`
     - Procedimiento almacenado "sys.table_exists": `EXECUTE`
   - Privilegios globales para todos los esquemas: `PROCESS`, `SUPER`

   Para crear una cuenta interna en el DBMS y otorgarle los privilegios necesarios, ejecute el siguiente script (en este script, el nombre de usuario es *KSCAdmin* y el nombre de la base de datos del Servidor de administración es *kav*):

```
/* Crear un usuario llamado KSCAdmin */
CREATE USER 'KSCAdmin'
/* Definir una contraseña para KSCAdmin */
IDENTIFIED BY '<contraseña>';
```

   Si utiliza MySQL 8.0 o anterior como DBMS, tenga en cuenta que para estas versiones no se admite la autenticación "Almacenamiento en caché de SHA2". Cambie la autenticación predeterminada de "Almacenamiento en caché de la contraseña SHA2" a "Contraseña nativa de MySQL".

   - Para crear en el DBMS una cuenta que utilice la autenticación nativa con contraseña de MySQL, ejecute el siguiente comando:

     `CREATE USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<contraseña>';`

   - Para cambiar el tipo de autenticación de una cuenta existente en el DBMS, ejecute el siguiente comando:

     `ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<contraseña>';`

```
/* Otorgar privilegios a KSCAdmin */
GRANT USAGE ON *.* TO 'KSCAdmin';
GRANT ALL ON kav.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';
GRANT PROCESS ON *.* TO 'KSCAdmin';
GRANT SUPER ON *.* TO 'KSCAdmin';
```

Si su DBMS es MariaDB versión 10.5 o anterior, no necesita otorgar el privilegio EXECUTE. En este caso, excluya el siguiente comando del script: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'`.

3. Para ver la lista de privilegios otorgados a la cuenta del DBMS, ejecute el siguiente script:

   ```
   SHOW grants for 'KSCAdmin';
   ```

4. Para crear manualmente la base de datos del Servidor de administración, ejecute el siguiente script (en este script, el nombre de la base de datos del Servidor de administración es *kav*):

   ```
   CREATE DATABASE kav
   DEFAULT CHARACTER SET ascii
   DEFAULT COLLATE ascii_general_ci;
   ```

   Utilice el mismo nombre para la base de datos que haya especificado en el script para crear la cuenta del DBMS.

5. Inicie sesión en el sistema con la cuenta de Windows que desee usar para ejecutar el instalador.

6. Ejecute el instalador.

   Se inicia el asistente de instalación del Servidor de administración. Siga las instrucciones del asistente.

7. Seleccione la opción de instalación personalizada del Servidor de administración.

8. Seleccione MySQL o MariaDB como DBMS que almacena la base de datos del Servidor de administración.

9. Especifique el nombre de la base de datos del Servidor de administración. Utilice el mismo nombre que en el script.

10. Especifique las credenciales de la cuenta de DBMS creada mediante el script.

11. Introduzca el nombre de la cuenta de Windows usada para iniciar el servicio del Servidor de administración.

    Puede seleccionar una cuenta de usuario de Windows existente o, mediante el instalador, crear automáticamente una nueva cuenta de Windows de formato KL-AK-*. En cualquiera de los dos casos, el instalador asignará los derechos del sistema necesarios a la cuenta utilizada para el servicio del Servidor de administración.

Una vez que concluya la instalación, se creará la base de datos del Servidor de administración y el Servidor de administración estará listo para usarse.

## Mover datos desde un espacio de tabla compartido a un espacio de tabla por archivo en un DBMS MySQL o MariaDB

Para un DBMS MySQL y MariaDB, puede almacenar datos de las siguientes maneras:

- Como espacio de tabla compartido, cuando los datos de todas las bases de datos de usuario se almacenan en un solo archivo (normalmente, en el archivo `ibdata1`).
- Como espacio de tabla de archivo por tabla, cuando para cada tabla se crea un espacio de datos separado como un archivo separado.

El uso de un espacio de tabla compartido aumenta el riesgo de fragmentación del espacio de tabla. Dado que no es posible realizar una operación `SHRINK`, un archivo en un espacio de tabla compartido puede ocupar aproximadamente el 90 % del espacio en disco. Esto afecta negativamente al rendimiento del subsistema de disco. Por lo tanto, es útil optar por un espacio de tabla de archivo por tabla.

En este artículo se describe cómo mover datos de un espacio de tabla compartido a un espacio de tabla de archivo por tabla. Si otras aplicaciones también utilizan el DBMS MySQL o MariaDB, debe mover las bases de datos de estas aplicaciones al espacio de tabla de archivo por tabla.

> Le recomendamos realizar el procedimiento solo si está utilizando DBMS MySQL o MariaDB para el Servidor de administración.
> Mover datos de un espacio de tabla compartido a un espacio de tabla de archivo por tabla puede aumentar la carga en el subsistema de disco.

## Requisitos previos

Antes de comenzar, asegúrese de lo siguiente:

- Creó una copia de seguridad de los datos del Servidor de administración ejecutando una tarea de copia de seguridad de datos o la utilidad klbackup.
- Creó una copia de seguridad de otras aplicaciones cuyas bases de datos están administradas con DBMS MySQL o MariaDB (si corresponde).
- En el dispositivo con el DBMS instalado, en la partición con la base de datos, hay espacio libre en disco.

El espacio en disco requerido es el 150% del tamaño total actual de las bases de datos (tamaño actual del `ibdata1` archivo).

## Proceso

*Para mover datos de un espacio de tabla compartido a un espacio de tabla de archivo por tabla:*

1. Detenga el servicio del Servidor de administración de Kaspersky Security Center y otras aplicaciones que utilicen la instancia del DBMS para la que desea realizar este procedimiento.

2. Dependiendo de la versión del DBMS, inicie sesión en su DBMS como superusuario y luego, en cualquier aplicación conveniente, ejecute el script `fix_tablespace.sql`.

   Puede ver los scripts `fix_tablespace.sql` haciendo clic en estos vínculos:

   Ver el script de MySQL 5.7 y MariaDB 10.1 o superiores

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;

    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';'
);
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;

        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

Ver el script para MySQL 8.0 o superiores

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;

    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';'
);
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;

        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` TABLESPACE =
innodb_file_per_table;' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt2;
        DEALLOCATE PREPARE stmt1;

        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

No debe detener la ejecución del script.
Si no se produjeron errores en el DBMS, pero finalizó la ejecución del script, vuelva a ejecutar el script o deje de realizar los pasos de este procedimiento, reinicie el servicio del DBMS y restaure los datos del Servidor de administración desde la copia de seguridad.

3. En la sección `[mysqld]` del archivo my.cnf, establezca el parámetro `innodb_file_per_table` en `1`.

4. Reinicie el servicio MySQL o MariaDB.

5. Inicie el servicio del Servidor de administración de Kaspersky Security Center.

Los datos se mueven de un espacio de tabla compartido a un espacio de tabla de archivo por tabla.

# Configurar las cuentas para trabajar con PostgreSQL y Postgres Pro

## Requisitos previos

Antes de asignar derechos a las cuentas, realice las siguientes acciones:

1. Inicie sesión en el sistema con la cuenta del administrador local.
2. Instale un entorno para trabajar con PostgreSQL y Postgres Pro.
3. Configure el servidor PostgreSQL o Postgres Pro para trabajar con Kaspersky Security Center 15.1.
4. Asegúrese de tener una cuenta de Windows que pueda usarse para instalar el Servidor de administración.
5. Asegúrese de tener una cuenta de Windows que pueda usarse para iniciar el servicio del Servidor de administración.

## Configuración de las cuentas para instalar el Servidor de administración (creación automática de la base de datos del Servidor de administración)

*Para configurar las cuentas para la instalación del Servidor de administración:*

1. Ejecute un entorno para trabajar con PostgreSQL y Postgres Pro.
2. Elija un rol de Postgres para acceder al DBMS. Puede usar cualquiera de los siguientes roles:
   - El usuario *Postgres* (el rol predeterminado de Postgres).

     Si usa el usuario *Postgres*, no es necesario que le conceda derechos adicionales.
   - Un nuevo rol de Postgres.

     Si prefiere utilizar un nuevo rol de Postgres, cree ese rol y concédale el privilegio CREATEDB. Para ello, ejecute el siguiente script (en este script, el rol es *KSCAdmin*):

     ```
     CREATE USER "KSCAdmin" WITH PASSWORD '<contraseña>' CREATEDB;
     ```

     El rol creado se utilizará como propietario de la base de datos del Servidor de administración (en adelante, también denominada "base de datos del Servidor").
3. Inicie sesión en el sistema en la cuenta de Windows utilizada para ejecutar el instalador del Servidor de administración (en adelante, también denominado instalador).
4. Ejecute el instalador.

   Se inicia el asistente de instalación del Servidor de administración. Siga las instrucciones del asistente.
5. Seleccione la opción de instalación personalizada del Servidor de administración.
6. Seleccione PostgreSQL o Postgres Pro como DBMS que almacena la base de datos del Servidor de administración.
7. Especifique el nombre de la base de datos del Servidor. El instalador creará automáticamente la base de datos del Servidor.

8. Especifique las credenciales del rol de Postgres.

9. Introduzca el nombre de la cuenta de Windows usada para iniciar el servicio del Servidor de administración.

   Puede seleccionar una cuenta de usuario de Windows existente o, mediante el instalador, crear automáticamente una nueva cuenta de Windows de formato KL-AK-*. En cualquiera de los dos casos, el instalador asignará los derechos del sistema necesarios a la cuenta utilizada para el servicio del Servidor de administración.

Una vez que concluya la instalación, se creará automáticamente la base de datos del Servidor de administración y el Servidor de administración estará listo para usarse.

## Configuración de las cuentas para instalar el Servidor de administración (creación manual de la base de datos del Servidor de administración)

*Para configurar las cuentas para la instalación del Servidor de administración:*

1. Ejecute un entorno para trabajar con Postgres.

2. Inicie sesión con el usuario *Postgres* en la base de datos *Postgres*.

3. Cree un nuevo rol de Postgres (en este ejemplo, el rol es *KSCAdmin*):

   ```
   CREATE USER "KSCAdmin" WITH PASSWORD '< contraseña >';
   ```

4. Cree una base de datos del Servidor de administración (en este ejemplo, el nombre de la base de datos del Servidor de administración es *KAV*):

   ```
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
   ```

   > Si aparece el error "La nueva codificación (UTF8) es incompatible con la codificación de la base de datos de plantilla", cree una base de datos mediante el comando:
   > `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin" TEMPLATE template0;`
   > en lugar de:
   > `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";`

5. Otórguele al rol todos los privilegios sobre la base de datos del Servidor de administración.

   ```
   GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
   ```

   > Asegúrese de que el rol tenga los privilegios CONNECT y TEMPORARY predeterminados en la base de datos del Servidor de administración.

6. Otorgue los siguientes privilegios al nuevo rol de Postgres:

   - Privilegios para todas las tablas del esquema "public": ALL
   - Privilegios para todas las secuencias del esquema "public": ALL

   Para hacer esto, inicie sesión con el usuario *Postgres* en la base de datos del *Servidor* y ejecute el siguiente script (en este script, el rol es *KSCAdmin*):

   ```
   GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";
   GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
   ```

7. Inicie sesión en el sistema con la cuenta de Windows que desee usar para ejecutar el instalador.
8. Ejecute el instalador del Servidor de administración.

   Se inicia el asistente de instalación del Servidor de administración. Siga las instrucciones del asistente.
9. Seleccione la opción de instalación personalizada del Servidor de administración.
10. Seleccione PostgreSQL o Postgres Pro como DBMS que almacena la base de datos del Servidor de administración.
11. Especifique el nombre de la base de datos del Servidor. Utilice el mismo nombre que en el script. Tenga en cuenta que el nombre de la base de datos distingue entre mayúsculas y minúsculas.
12. Especifique las credenciales del rol de Postgres.
13. Introduzca el nombre de la cuenta de Windows usada para iniciar el servicio del Servidor de administración.

    Puede seleccionar una cuenta de usuario de Windows existente o, mediante el instalador, crear automáticamente una nueva cuenta de Windows de formato KL-AK-*. En cualquiera de los dos casos, el instalador asignará los derechos del sistema necesarios a la cuenta utilizada para el servicio del Servidor de administración.

Una vez que concluya la instalación, el Servidor de administración utilizará la base de datos creada para almacenar los datos del Servidor de administración. El Servidor de administración estará entonces listo para usar.

# Escenario: autenticación de Microsoft SQL Server

La información de esta sección solo corresponde a las configuraciones en las que Kaspersky Security Center utiliza Microsoft SQL Server como el sistema de administración de bases de datos.

Para proteger los datos de Kaspersky Security Center transferidos hacia la base de datos o desde esta y aquellos almacenados en la base de datos contra el acceso no autorizado, debe asegurar la comunicación entre Kaspersky Security Center y SQL Server. La forma más confiable de garantizar una comunicación segura es instalar Kaspersky Security Center y SQL Server en el mismo dispositivo y usar el mecanismo de memoria compartida para ambas aplicaciones. En los demás casos, le recomendamos que use un certificado SSL o TLS para autenticar la instancia de SQL Server. Puede usar un certificado de una autoridad de certificación (AC) de confianza o un certificado autofirmado. Los certificados emitidos por las AC son preferibles a los autofirmados; estos últimos brindan un nivel de protección limitado.

La autenticación de SQL Server procede en etapas:

1. **Generación de un certificado SSL o TLS autofirmado para SQL Server de acuerdo con los requisitos del certificado**

   Si ya tiene un certificado para SQL Server, omita este paso.

   Un certificado SSL solo puede usarse en las versiones de SQL Server anteriores a 2016 (13.x). En SQL Server 2016 (13.x) y versiones posteriores, use un certificado TLS.

   Para generar un certificado TLS, ejecute (por ejemplo) el siguiente comando en PowerShell:

   ```
   New-SelfSignedCertificate -DnsName SQL_HOST_NAME -CertStoreLocation cert:\LocalMachine
   -KeySpec KeyExchange
   ```

Antes de ejecutar el comando, asegúrese de reemplazar la cadena SQL_HOST_NAME con el nombre de host del servidor SQL Server (si el host pertenece al dominio) o con el nombre de dominio completo (*FQDN*) del servidor si el host no forma parte del dominio. Se debe especificar el mismo nombre (nombre del host o FQDN) como nombre de la instancia de SQL Server en el Asistente de instalación del Servidor de administración.

2. **Adición del certificado en la instancia de SQL Server**

   Las instrucciones para completar esta etapa varían según la plataforma en la que se ejecuta SQL Server. Para obtener más información, consulte la documentación oficial:

   - Windows
   - Linux
   - Amazon Relational Database Service
   - Windows Azure

   Para usar el certificado en un clúster de conmutación por error, debe instalar el certificado en cada nodo de este clúster. Para obtener más información, consulte la documentación de Microsoft.

3. **Asignación de los permisos de la cuenta de servicio**

   Asegúrese de que la cuenta de servicio en la cual se ejecuta el servicio de SQL Server tenga el permiso de control total para acceder a las claves privadas. Para obtener más información, consulte la documentación de Microsoft.

4. **Adición del certificado a la lista de certificados de confianza para Kaspersky Security Center**

   En el dispositivo del Servidor de administración, agregue el certificado a la lista de certificados de confianza. Para obtener más información, consulte la documentación de Microsoft.

5. **Activación de conexiones cifradas entre la instancia de SQL Server y Kaspersky Security Center**

   En el dispositivo del Servidor de administración, establezca el valor `1` en la variable de entorno `KLDBADO_UseEncryption`. Por ejemplo, en Windows Server 2012 R2, puede cambiar las variables del entorno haciendo clic en **Variables de entorno** en la pestaña **Avanzado** de la ventana **Propiedades del sistema**. Agregue una nueva variable, asígnele el nombre `KLDBADO_UseEncryption` y luego establezca el valor `1`.

6. **Configuración adicional para usar el protocolo TLS 1.2**

   Si usa el protocolo TLS 1.2, además haga lo siguiente:

   - Asegúrese de que la versión instalada de SQL Server sea una aplicación de 64 bits.
   - Instale el controlador de OLE DB de Microsoft en el dispositivo del Servidor de administración. Para obtener más información, consulte la documentación de Microsoft.
   - En el dispositivo del Servidor de administración, establezca el valor `1` en la variable de entorno `KLDBADO_UseMSOLEDBSQL`. Por ejemplo, en Windows Server 2012 R2, puede cambiar las variables del entorno haciendo clic en **Variables de entorno** en la pestaña **Avanzado** de la ventana **Propiedades del sistema**. Agregue una nueva variable, asígnele el nombre `KLDBADO_UseMSOLEDBSQL` y luego establezca el valor `1`.

     Si la versión del controlador OLE DB es 19 o más reciente, establezca también el valor `MSOLEDBSQL19` a la variable de entorno `KLDBADO_ProviderName` .

7. **Activación del uso del protocolo TCP/IP en una instancia con nombre de SQL Server**

Si usa una instancia con nombre de SQL Server, además habilite el uso del protocolo TCP/IP y asigne un número de puerto TCP/IP al motor de base de datos de SQL Server. Cuando configure la conexión de SQL Server en el Asistente de instalación del Servidor de administración, especifique el nombre del host de SQL Server y el número del puerto en el campo **Nombre de la instancia de SQL Server**.

# Escenario: autenticación del servidor MySQL

Le recomendamos que utilice un certificado TLS para autenticar el servidor MySQL. Puede usar un certificado de una autoridad de certificación (AC) de confianza o un certificado autofirmado.

El Servidor de administración admite autenticación SSL unidireccional y bidireccional para MySQL.

## Habilitación de la autenticación SSL unidireccional

Siga estos pasos a fin de configurar la autenticación SSL unidireccional para MySQL:

1. **Genere un certificado TLS autofirmado para el servidor MySQL**

   En PowerShell, cambie el directorio a la carpeta donde desea almacenar los certificados. Ejecute los siguientes comandos:

```
$CertCA = New-SelfSignedCertificate `
-Subject "CN=CertCA" `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm "SHA256" `
-NotAfter (Get-Date).AddDays(365)

$CertCABase64 = [System.Convert]::ToBase64String($CertCA.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertLeaf = New-SelfSignedCertificate `
-Subject "CN=CertLeaf" `
–Signer $CertCA `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm" SHA256
-KeyExportPolicy Exportable `
-NotAfter (Get-Date).AddDays(365)

$CertLeafBase64 = [System.Convert]::ToBase64String($CertLeaf.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)

$ CertLeafRSACng = [System.Security.Cryptography.X509Certificates.RSACertificateExtensions] :: GetRSAPrivateKey
($ CertLeaf)
$ CertLeafKeyBytes = $ SystemLeafRSACng CngKeyBlobFormat] :: Pkcs8PrivateBlob)
$CertLeafKeyBase64 = [System.Convert]::ToBase64String($CertLeafKeyBytes,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertCAPemCert = @"
-----BEGIN CERTIFICATE-----
$ CertCABase64
-----END CERTIFICATE-----
"@

$CertLeafPemKey = @"
-----BEGIN PRIVATE KEY-----
$ CertLeafKeyBase64
-----END PRIVATE KEY-----
"@

$CertLeafPemCert = @"
-----BEGIN CERTIFICATE-----
$ CertLeafBase64
-----END CERTIFICATE-----
"@

# Output to file

$CertCAPemCert | Out-File -FilePath ca-cert.pem -Encoding Ascii
```

```
$CertLeafPemKey | Out-File -FilePath server-key.pem -Encoding Ascii
$CertLeafPemCert | Out-File -FilePath server-cert.pem -Encoding Ascii
```

Estos comandos crean certificados para el usuario actual y exportan los certificados al formato PEM. Solo necesita los archivos PEM exportados para autenticar el servidor. Para eliminar los certificados creados de Windows, ejecute el siguiente comando en PowerShell:

```
certmgr.msc
```

Busque los certificados creados en la carpeta **Personal** → **Certificados** y elimínelos.

2. **Cree un archivo de indicador del servidor**

   Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada es <Disk>:\Archivos de programa(x86)\Kaspersky Lab\Kaspersky Security Center.

   Use la utilidad klscflag para crear el indicador del servidor KLSRV_MYSQL_OPT_SSL_CA y especifique la ruta al certificado como su valor:

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <ruta a ca-cert.pem> -t s
   ```

3. **Configure las bases de datos**

   Especifique los certificados en el archivo my.cnf. Abra el archivo my.cnf en un editor de texto y agregue las siguientes líneas en la sección [mysqld]:

   ```
   [mysqld]
   ssl-ca="...\mysqlcerts\ca-cert.pem"
   ssl-cert="...\mysqlcerts\server-cert.pem"
   ssl-key="...\mysqlcerts\server-key.pem"
   ```

## Habilitación de la autenticación SSL bidireccional

Siga estos pasos a fin de configurar la autenticación SSL bidireccional para MySQL:

1. **Cree archivos de indicador del servidor**

   Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada es <Disk>:\Archivos de programa(x86)\Kaspersky Lab\Kaspersky Security Center.

   Use la utilidad klscflag para crear indicadores del servidor y especifique la ruta a los archivos de certificados como sus valores:

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <ruta a ca-cert.pem> -t s
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <ruta a server-cert.pem> -t
   s
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <ruta a server-key.pem> -t s
   ```

2. **Especifique la frase de contraseña (opcional)**

   Si server-key.pem requiere una frase de contraseña, cree un indicador KLSRV_MARIADB_OPT_TLS_PASPHRASE y especifique la frase de contraseña como su valor:

```
klscflag -fset -pv klserver -n KLSRV_MARIADB_OPT_TLS_PASPHRASE -v <frase de contraseña>
-t s
```

3. **Configure las bases de datos**

   Especifique los certificados en el archivo my.cnf. Abra el archivo my.cnf en un editor de texto y agregue las siguientes líneas en la sección [mysqld]:

   ```
   [mysqld]

   ssl-ca="...\ca-cert.pem"

   ssl-cert="...\server-cert.pem"

   ssl-key="...\server-key.pem"
   ```

# Escenario: autenticación del servidor PostgreSQL

Le recomendamos que utilice un certificado TLS para autenticar el servidor PostgreSQL. Puede usar un certificado de una autoridad de certificación (AC) de confianza o un certificado autofirmado. Use certificados emitidos por una AC confiable, ya que los autofirmados brindan un nivel de protección limitado.

El Servidor de administración admite autenticación SSL unidireccional y bidireccional para PostgreSQL.

La autenticación del servidor PostgreSQL se realiza por etapas:

1. **Generar un certificado para el servidor PostgreSQL**

   En una utilidad multiplataforma basada en OpenSSL, ejecute los siguientes comandos:

   ```
   openssl req -new -x509 -days 365 -nodes -text -out psql.crt -keyout psql.key -subj
   "/CN=psql"

   chmod og-rwx psql.key
   ```

2. **Generar un certificado para el Servidor de administración**

   Ejecute los siguientes comandos. El valor CN debe coincidir con el nombre del usuario que se conecta a PostgreSQL en nombre del Servidor de administración. El nombre de usuario está configurado en postgres de manera predeterminada.

   ```
   openssl req -new -x509 -days 365 -nodes -text -out postgres.crt -keyout postgres.key -
   subj "/CN=postgres"

   chmod og-rwx postgres.key
   ```

3. **Configurar la autenticación del certificado del cliente**

   Modifique pg_hba.conf de la siguiente manera:

   ```
   hostssl all all 0.0.0.0/0 md5
   ```

   Asegúrese de que pg_hba.conf no incluya un registro que comience con `host`.

4. **Especificar el certificado del servidor PostgreSQL**

   Autenticación SSL unidireccional

Modifique postgresql.conf de la siguiente manera (especifique la ruta correcta a los archivos .crt y .key):

```
listen_addresses ='localhost, server-ip'
ssl = on
ssl_cert_file = '<psql.crt>'
ssl_key_file = '<psql.key>'
```

Autenticación SSL bidireccional

Modifique postgresql.conf de la siguiente manera (especifique la ruta correcta a los archivos .crt y .key):

```
listen_addresses ='localhost, server-ip'
ssl = on
ssl_ca_file = '<postgres.crt>'
ssl_cert_file = '<psql.crt>'
ssl_key_file = '<psql.key>'
```

5. **Reiniciar el servicio en segundo plano PostgreSQL**

   Ejecute el siguiente comando:

   ```
   systemctl restart postgresql-14.service
   ```

6. **Especificar el indicador de servidor para el Servidor de administración**

   Autenticación SSL unidireccional

   Use la utilidad klscflag para crear el indicador del servidor KLSRV_POSTGRES_OPT_SSL_CA y especifique la ruta al certificado como su valor:

   Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada es <Disk>:\Archivos de programa(x86)\Kaspersky Lab\Kaspersky Security Center.

   Ejecute el siguiente comando:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <ruta a psql.crt> -t s
   ```

   Autenticación SSL bidireccional

Use la utilidad klscflag para crear indicadores del servidor y especifique la ruta a los archivos de certificados como sus valores.

Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada es <Disk>:\Archivos de programa(x86)\Kaspersky Lab\Kaspersky Security Center.

Ejecute el siguiente comando:

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <ruta a psql.crt> -t s
```

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v <ruta a postgres.crt> -t s
```

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v <ruta a postgres.key> -t s
```

Si `postgres.key` requiere una frase de contraseña, cree un indicador KLSRV_POSTGRES_OPT_TLS_PASPHRASE y especifique la frase de contraseña como su valor:

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v <frase de contraseña> -t s
```

7. **Reiniciar el servicio del Servidor de administración**

# Recomendaciones sobre la instalación del Servidor de administración

Esta sección contiene recomendaciones sobre cómo para instalar el Servidor de administración. Esta sección también proporciona situaciones sobre cómo usar una carpeta compartida en el dispositivo del Servidor de administración a fin de instalar el Agente de red en los dispositivos cliente.

## Creación de cuentas para los servicios del Servidor de administración en un clúster de conmutación por error

De forma predeterminada, el instalador automáticamente crea cuentas no privilegiadas para servicios del Servidor de administración. Este comportamiento es el más conveniente para la instalación del Servidor de administración en un dispositivo común.

Sin embargo, la instalación del Servidor de administración en un clúster de conmutación por error requiere una situación diferente:

1. Crear cuentas de dominio sin privilegios para los servicios del Servidor de administración convertirlas en miembros del grupo de seguridad de dominio global llamado KLAdmins.

2. En el instalador del Servidor de administración, especificar las cuentas de dominio que se han creado para los servicios.

## Definición de una carpeta compartida

Al instalar el Servidor de administración, puede especificar la ubicación de la carpeta compartida. También puede especificar la ubicación de la carpeta compartida después de la instalación, en las propiedades del Servidor de administración. De forma predeterminada, la carpeta compartida se creará en el dispositivo con el Servidor de administración (con derechos de lectura para el subgrupo **Todos**). Sin embargo, en algunos casos (como cuando hay carga alta o se debe acceder desde una red aislada, etc.), es útil localizar la carpeta compartida en un recurso de archivo dedicado.

La carpeta compartida se utiliza en ocasiones para realizar el despliegue del Agente de red.

Se debe desactivar la distinción entre mayúsculas y minúsculas para la carpeta compartida.

## Instalación remota con herramientas del Servidor de administración a través de directivas de grupo de Active Directory

Si los dispositivos de destino se encuentran en un dominio de Windows (sin grupos de trabajo), el despliegue inicial (la instalación del Agente de red y de la aplicación de seguridad en los dispositivos que aún no son administrados) se tiene que realizar a través de directivas de grupo de Active Directory. La distribución se realiza usando la tarea estándar para la instalación remota de Kaspersky Security Center. Si la red es a gran escala, resulta útil localizar la carpeta compartida en un recurso del archivo dedicado para reducir la carga en el subsistema del disco del dispositivo del Servidor de administración.

## Instalación remota a través de la distribución de la ruta de UNC a un paquete independiente

Si los usuarios de los dispositivos conectados a la red de la organización tienen derechos de administrador local, otro método para realizar el despliegue inicial es crear un paquete independiente para el Agente de red (o incluso un paquete "combinado", que contenga tanto el Agente de red como la aplicación de seguridad). Después de crear un paquete independiente, envíe a los usuarios un enlace a ese paquete, que se almacena en la carpeta compartida. La Instalación se inicia cuando los usuarios hacen clic en el enlace.

## Actualización desde la carpeta compartida del Servidor de administración

En la tarea de actualización del antivirus, puede configurar la actualización desde la carpeta compartida del Servidor de administración. Si la tarea se ha asignado a un gran número de dispositivos, es útil localizar la carpeta compartida en un recurso del archivo dedicado.

## Instalación de imágenes de los sistemas operativos

Las imágenes del sistema operativo siempre se instalan a través de la carpeta compartida: los dispositivos leen imágenes del sistema operativo desde la carpeta compartida. Si planea instalar las imágenes en un gran número de dispositivos corporativos, recomendamos que la carpeta compartida se encuentre en un recurso de archivos dedicado.

## Especificación de la dirección del Servidor de administración

Al instalar el Servidor de administración, puede especificar la dirección del equipo que alberga el Servidor de administración. Esta dirección se utilizará como dirección predeterminada al crear paquetes de instalación del Agente de red.

Como dirección del Servidor de administración, puede especificar lo siguiente:

- Nombre NetBIOS del Servidor de administración, que se especifica de forma predeterminada.
- Nombre de dominio completo (FQDN) del Servidor de administración si se configuró el Sistema de nombres de dominio (DNS) en la red de la organización y funciona correctamente.
- Dirección externa si el Servidor de administración está instalado en la zona desmilitarizada (DMZ).

Después de esto, podrá cambiar la dirección del Servidor de administración usando las herramientas de la Consola de administración. La dirección no cambiará automáticamente en los paquetes de instalación del Agente de red que ya se hayan creado.

# Instalación estándar

La instalación estándar es una instalación del Servidor de administración que usa las rutas predeterminadas para los archivos de aplicación, instala el conjunto predeterminado de complementos y no habilita la Administración de dispositivos móviles.

*Para instalar del Servidor de administración de Kaspersky Security Center en un dispositivo local:*

Ejecute el archivo ejecutable ksc_<número de versión>.<número de compilación>_full_<idioma de localización>.exe.

Se abre una ventana y se le solicita que seleccione las aplicaciones de Kaspersky que desea instalar. En la ventana de selección de aplicaciones, haga clic en el enlace **Instalar del Servidor de administración de Kaspersky Security Center** para ejecutar el asistente de instalación del Servidor de administración. Siga las instrucciones del asistente.

## Paso 1. Revisar el Contrato de licencia y la Política de privacidad

En esta etapa del Asistente de instalación, debe leer el Contrato de licencia, que se establecerá entre usted y Kaspersky, así como la Política de privacidad.

También se le puede solicitar que vea los Contratos de licencia y las Políticas de privacidad para los complementos de administración de aplicaciones que están disponibles en el kit de distribución de Kaspersky Security Center.

Por favor lea con atención el Contrato de licencia y la Política de privacidad. Si está de acuerdo con todos los términos del Contrato de licencia y la Política de privacidad, confírmelo seleccionando las casillas de verificación correspondientes.

La instalación de la aplicación en su dispositivo continuará después de que seleccione ambas casillas.

Si no acepta el Contrato de licencia o la Política de privacidad, cancele la instalación haciendo clic en el botón **Cancelar**.

## Paso 2. Seleccionar el método de instalación

En la ventana de selección del tipo de instalación, seleccione **Estándar**.

Se recomienda la instalación estándar si desea probar Kaspersky Security Center, por ejemplo, al probar su funcionamiento en un área pequeña dentro su red empresarial. Durante la instalación estándar, solo se configura la base de datos. No especifica ninguna configuración del Servidor de administración: en cambio, se utilizan sus respectivos valores predeterminados. La instalación estándar no permite seleccionar complementos de administración para instalar; solo se instala el conjunto predeterminado de complementos. Durante la instalación estándar, no se crea ningún paquete de instalación para dispositivos móviles. Sin embargo, puede crearlos más adelante en la Consola de administración.

## Paso 3. Instalación de Kaspersky Security Center Web Console

Este paso se muestra solo si está utilizando un sistema operativo de 64 bits. De lo contrario, este paso no se muestra, porque Kaspersky Security Center Web Console no funciona con sistemas operativos de 32 bits.

De forma predeterminada, se instalarán tanto Kaspersky Security Center Web Console como la Consola de administración basada en MMC.

*Si solo desea instalar Kaspersky Security Center Web Console, siga estos pasos:*

1. Seleccione **Instalar solo este**.
2. Elija **Consola basada en la Web** en la lista desplegable.

La instalación de Kaspersky Security Center Web Console se inicia automáticamente después de completar la instalación del Servidor de administración.

*Si desea instalar solo la Consola de administración basada en MMC:*

1. Seleccione **Instalar solo este**.
2. Elija **Consola basada en MMC** en la lista desplegable.

## Paso 4. Seleccionar el tamaño de la red

Especifique la escala de la red en la cual instalará Kaspersky Security Center. Según el número de dispositivos en la red, el asistente configura la instalación y el aspecto de la interfaz de la aplicación para que coincidan.

La siguiente tabla enumera la configuración de instalación de la aplicación y la configuración de la apariencia de la interfaz que se ajustan basadas en varios tamaños de red.

Correspondencia de la configuración de instalación con el tamaño de red seleccionado

| Configuración | De 1 a 100 dispositivos administrados | De 101 a 1000 dispositivos administrados | De 1001 a 5000 dispositivos administrados | Más de 5000 dispositivos administrados |
|---|---|---|---|---|
| Mostrar con el nodo de los Servidores de administración secundarios y virtuales y todos los parámetros de configuración relacionados con estos servidores en el árbol de consola (solo disponible en la Consola de administración basada en MMC) | No disponible | No disponible | Disponible | Disponible |
| Mostrar con las secciones **Seguridad** en las ventanas de propiedades del Servidor de administración y grupos de administración (solo disponible en la Consola de administración basada en MMC) | No disponible | No disponible | Disponible | Disponible |
| Distribuir aleatoriamente el tiempo de inicio de la tarea de actualización en los dispositivos cliente | No disponible | Sobre un intervalo de 5 minutos | Sobre un intervalo de 10 minutos | Sobre un intervalo de 10 minutos |

Si conecta el Servidor de administración a un servidor de bases de datos MySQL 5.7 o SQL Express, recomendamos que no use la aplicación para administrar más de 10 000 dispositivos. Para el servidor de bases de datos MariaDB, el máximo recomendado es de 20000 dispositivos administrados.

## Paso 5. Seleccionar una base de datos

En este paso del asistente, seleccione uno de los siguientes sistemas de gestión de bases de datos (DBMS) que se utilizará para almacenar la base de datos del Servidor de administración:

- **Microsoft SQL Server o SQL Server Express**
- **MySQL o MariaDB**
- **PostgreSQL o Postgres Pro**

Se recomienda instalar el Servidor de administración en un servidor dedicado y no en un controlador de dominio. Sin embargo, si instala Kaspersky Security Center en un servidor que actúe como controlador de dominio de solo lectura (RODC), Microsoft SQL Server (SQL Express) no se debe instalar de manera local (en el mismo dispositivo). En este caso, le recomendamos que instale Microsoft SQL Server (SQL Express) de forma remota (en un dispositivo diferente) o que use MySQL, MariaDB o PostgreSQL si necesita instalar el DBMS de manera local.

La estructura de la base de datos del Servidor de administración se proporciona en el archivo klakdb.chm, que se encuentra en la carpeta de instalación de Kaspersky Security Center. Este archivo también está disponible en un archivo en el portal de Kaspersky: klakdb.zip.

# Paso 6. Configurar el Servidor SQL

En este paso del asistente, especifique la siguiente configuración de conexión, según el sistema de administración de bases de datos (DBMS) que haya seleccionado:

- Si seleccionó **Microsoft SQL Server o SQL Server Express** en el paso anterior:

  - En el campo **Instancia de SQL Server**, especifique el nombre de SQL Server en la red. Para ver una lista de todas las instancias de SQL Server que estén en la red, haga clic en el botón **Examinar**. Este campo aparece en blanco de forma predeterminada.

    Si utiliza un puerto distinto del estándar para conectarse a SQL Server, indique el número de puerto junto con el nombre del host de SQL Server, separando los dos datos con una coma. Por ejemplo:

    ```
    nombre_host_SQL_Server, 1433
    ```

    Si utiliza un certificado para proteger las comunicaciones entre el Servidor de administración y SQL Server, asegúrese de que el nombre de host que escriba en el campo **Instancia de SQL Server** sea el mismo que haya utilizado para generar el certificado. Si utiliza una instancia con nombre de SQL Server, junto con el nombre del host de SQL Server, especifique el número del puerto separado con una coma, por ejemplo:

    ```
    nombre_SQL_Server, 1433
    ```

    Si usa varias instancias de SQL Server en el mismo host, especifique además el nombre de la instancia separado con una barra diagonal inversa, por ejemplo:

    ```
    nombre_SQL_Server\nombre_instancia_SQL_Server, 1433
    ```

    Si un SQL Server en la red empresarial tiene habilitada la característica Always On, especifique el nombre del oyente del grupo de disponibilidad en el campo **Instancia de SQL Server**. Tenga en cuenta que el Servidor de administración solo admite el modo de disponibilidad de confirmación sincrónica cuando la característica Always On está habilitada.

  - En el campo **Nombre de la base de datos**, especifique el nombre de la base de datos que se creará para almacenar los datos del Servidor de administración. El valor predeterminado es *KAV*.

  Si en esta etapa desea instalar SQL Server en el dispositivo desde el cual está instalando Kaspersky Security Center, debe detener la instalación y reiniciarla después de la instalación de SQL Server. Las versiones compatibles de SQL Server figuran en los requisitos del sistema.

  Si está instalando SQL Server en un dispositivo remoto, no es preciso interrumpir el asistente de instalación de Kaspersky Security Center. Instale el servidor SQL Server y luego continúe con la instalación de Kaspersky Security Center.

- Si seleccionó **MySQL o MariaDB** en el paso anterior:

  - En el campo **Instancia de SQL Server**, especifique el nombres de la instancia de DBMS. De forma predeterminada, el nombre es la dirección IP del dispositivo en el cual se debe instalar Kaspersky Security Center.

  - En el campo **Puerto**, especifique el puerto para la conexión del Servidor de administración con el DBMS. El número de puerto predeterminado es 3306.

  - En el campo **Nombre de la base de datos**, especifique el nombre de la base de datos que se creará para almacenar los datos del Servidor de administración. El valor predeterminado es *KAV*.

- Si seleccionó **PostgreSQL o Postgres Pro** en el paso anterior:

- En el campo **Servidor PostgreSQL o Postgres Pro**, especifique el nombre de la instancia de DBMS. De forma predeterminada, el nombre es la dirección IP del dispositivo en el cual se debe instalar Kaspersky Security Center.

- En el campo **Puerto**, especifique el puerto para la conexión del Servidor de administración con el DBMS. El número de puerto predeterminado es 5432.

- En el campo **Nombre de la base de datos**, especifique el nombre de la base de datos que se creará para almacenar los datos del Servidor de administración. El valor predeterminado es *KAV*.

## Paso 7. Seleccionar el modo de autenticación

Determine el modo de autenticación que se utilizará cuando el Servidor de administración se conecte con el sistema de administración de bases de datos (DBMS).

Según el DBMS seleccionado, puede elegir entre los siguientes modos de autenticación:

- Para el servidor SQL Express o Microsoft SQL Server, seleccione una de las siguientes opciones:

  - **Modo de autenticación de Microsoft Windows**. La verificación de permisos usa la cuenta utilizada para el inicio del Servidor de administración.

  - **Modo de autenticación de SQL Server**. Si selecciona esta opción, la cuenta especificada en la ventana se usa para verificar los permisos de acceso. Rellene los campos **Cuenta** y **Contraseña**.

    Para ver la contraseña introducida, haga clic y mantenga presionado el botón **Mostrar**.

  Para ambos modos de autenticación, la aplicación comprueba si la base de datos está disponible. Si la base de datos no está disponible, se muestra un mensaje de error y debe proporcionar las credenciales correctas.

  Si la base de datos del Servidor de administración se almacena en otro dispositivo y la cuenta del Servidor de administración no tiene el acceso al servidor de la base de datos, debe usar el modo de autenticación de SQL Server al instalar o actualizar el Servidor de administración. Esto puede ocurrir cuando el dispositivo que almacena la base de datos se encuentra fuera del dominio o cuando el Servidor de administración está instalado en la cuenta LocalSystem.

- Para MySQL, MariaDB, PostgreSQL o Postgres Pro, especifique la cuenta y la contraseña.

## Paso 8. Desempaquetar e instalar archivos en el disco duro

Después de configurar la instalación de los componentes de Kaspersky Security Center, puede comenzar con la instalación de archivos en el disco duro.

Si la instalación requiere programas adicionales, el asistente de instalación se lo notificará en la página **Instalando requisitos previos** antes de instalar Kaspersky Security Center. Los programas requeridos se instalarán automáticamente después de hacer clic en el botón **Siguiente**.

En la última página, puede seleccionar qué consola desea iniciar para trabajar con Kaspersky Security Center:

- **Iniciar Consola de administración basada en MMC**
- **Iniciar Kaspersky Security Center Web Console**

  Esta opción solo está disponible si ha optado por instalar Kaspersky Security Center Web Console en uno de los pasos anteriores.

También puede hacer clic en **Finalizar** para cerrar el asistente sin comenzar a trabajar con Kaspersky Security Center. Puede iniciar el trabajo más tarde en cualquier momento.

Al iniciar por primera vez la Consola de administración o Kaspersky Security Center Web Console, puede realizar la configuración inicial de la aplicación.

Cuando el Asistente de instalación finaliza, los siguientes componentes de la aplicación se instalan en el disco duro en el cual se ha instalado el sistema operativo:

- Servidor de administración (junto con la versión de servidor del Agente de red).
- Consola de administración basada en Microsoft Management Console.
- Kaspersky Security Center Web Console (si decidiera instalarlo).
- Los complementos de administración de aplicaciones se encuentran disponibles en el kit de distribución.

Además, se instalará Microsoft Windows Installer 4.5 si no se instaló anteriormente.

# Instalación personalizada

La instalación personalizada es una instalación del Servidor de administración durante la cual se le solicita seleccionar componentes para instalar y especificar la carpeta en la cual se debe instalar la aplicación.

Al usar este tipo de la instalación, puede configurar la base de datos y el Servidor de administración, así como instalar componentes que no están incluidos en la instalación estándar o los complementos de administración para varias aplicaciones de seguridad de Kaspersky. También puede habilitar la Administración de dispositivos móviles.

*Para instalar del Servidor de administración de Kaspersky Security Center en un dispositivo local:*

Ejecute el archivo ejecutable ksc_<número de versión>.<número de compilación>_full_<idioma de localización>.exe.

Se abre una ventana y se le solicita que seleccione las aplicaciones de Kaspersky que desea instalar. En la ventana de selección de aplicaciones, haga clic en el enlace **Instalar del Servidor de administración de Kaspersky Security Center** para ejecutar el asistente de instalación del Servidor de administración. Siga las instrucciones del asistente.

## Paso 1. Revisar el Contrato de licencia y la Política de privacidad

En esta etapa del Asistente de instalación, debe leer el Contrato de licencia, que se establecerá entre usted y Kaspersky, así como la Política de privacidad.

También se le puede solicitar que vea los Contratos de licencia y las Políticas de privacidad para los complementos de administración de aplicaciones que están disponibles en el kit de distribución de Kaspersky Security Center.

Por favor lea con atención el Contrato de licencia y la Política de privacidad. Si está de acuerdo con todos los términos del Contrato de licencia y la Política de privacidad, confírmelo seleccionando las casillas de verificación correspondientes.

La instalación de la aplicación en su dispositivo continuará después de que seleccione ambas casillas.

Si no acepta el Contrato de licencia o la Política de privacidad, cancele la instalación haciendo clic en el botón **Cancelar**.

## Paso 2. Seleccionar el método de instalación

En la ventana de selección del tipo de instalación, especifique **Personalizada**.

La instalación personalizada le permite modificar la configuración de Kaspersky Security Center, como la ruta a la carpeta compartida, las cuentas y los puertos para la conexión con el Servidor de administración, y la configuración de la base de datos. La instalación personalizada le permite especificar qué complementos de administración de Kaspersky instalar. Durante la instalación personalizada, puede crear paquetes de instalación para dispositivos móviles al habilitar la opción correspondiente.

## Paso 3. Seleccionar los componentes a instalar

Seleccione los componentes del Servidor de administración de Kaspersky Security Center que desee instalar:

- **Administración de dispositivos móviles**. Seleccione esta casilla de verificación si debe crear paquetes de instalación para dispositivos móviles cuando se esté ejecutando el asistente de instalación de Kaspersky Security Center. También puede crear paquetes de instalación para dispositivos móviles manualmente, después de la instalación del Servidor de administración, utilizando las herramientas de la Consola de administración.

- **Agente SNMP**. Este componente recibe la información estadística para el Servidor de administración a través del protocolo SNMP. El componente solamente está disponible si la aplicación se instala en un dispositivo con SNMP instalado.

  Después de instalar Kaspersky Security Center, los archivos .mib requeridos para recibir estadísticas se ubicarán en la subcarpeta SNMP de la carpeta de instalación de la aplicación.

El Agente de red y la Consola de administración no se muestran en la lista de componentes. Estos componentes se instalan de manera automática y no se puede cancelar su instalación.

En este paso, debe especificar una carpeta para instalar los componentes del Servidor de administración. De manera predeterminada, los componentes se instalan en <Disco>:\Archivos de programa\Kaspersky Lab\Kaspersky Security Center. Si no existe la carpeta, se crea en forma automática durante la instalación. Es posible cambiar la carpeta de destino usando el botón **Examinar**.

## Paso 4. Instalación de Kaspersky Security Center Web Console

Este paso se muestra solo si está utilizando un sistema operativo de 64 bits. De lo contrario, este paso no se muestra, porque Kaspersky Security Center Web Console no funciona con sistemas operativos de 32 bits.

De forma predeterminada, se instalarán tanto Kaspersky Security Center Web Console como la Consola de administración basada en MMC.

*Si solo desea instalar Kaspersky Security Center Web Console, siga estos pasos:*

1. Seleccione **Instalar solo este**.
2. Elija **Consola basada en la Web** en la lista desplegable.

La instalación de Kaspersky Security Center Web Console se inicia automáticamente después de completar la instalación del Servidor de administración.

*Si desea instalar solo la Consola de administración basada en MMC:*

1. Seleccione **Instalar solo este**.
2. Elija **Consola basada en MMC** en la lista desplegable.

## Paso 5. Seleccionar el tamaño de la red

Especifique la escala de la red en la cual instalará Kaspersky Security Center. Según el número de dispositivos en la red, el asistente configura la instalación y el aspecto de la interfaz de la aplicación para que coincidan.

La siguiente tabla enumera la configuración de instalación de la aplicación y la configuración de la apariencia de la interfaz que se ajustan basadas en varios tamaños de red.

Correspondencia de la configuración de instalación con el tamaño de red seleccionado

| Configuración | De 1 a 100 dispositivos administrados | De 101 a 1000 dispositivos administrados | De 1001 a 5000 dispositivos administrados | Más de 5000 dispositivos administrados |
|---|---|---|---|---|
| Mostrar con el nodo de los Servidores de administración secundarios y virtuales y todos los parámetros de configuración relacionados con estos servidores en el árbol de consola (solo disponible en la Consola de administración basada en MMC) | No disponible | No disponible | Disponible | Disponible |
| Mostrar con las secciones **Seguridad** en las ventanas de propiedades del Servidor de administración y grupos de administración (solo disponible en la Consola de administración basada en MMC) | No disponible | No disponible | Disponible | Disponible |
| Distribuir aleatoriamente el tiempo de inicio de la tarea de actualización en los dispositivos cliente | No disponible | Sobre un intervalo de 5 minutos | Sobre un intervalo de 10 minutos | Sobre un intervalo de 10 minutos |

Si conecta el Servidor de administración a un servidor de bases de datos MySQL 5.7 o SQL Express, recomendamos que no use la aplicación para administrar más de 10 000 dispositivos. Para el servidor de bases de datos MariaDB, el máximo recomendado es de 20000 dispositivos administrados.

## Paso 6. Seleccionar una base de datos

En este paso del asistente, seleccione uno de los siguientes sistemas de gestión de bases de datos (DBMS) que se utilizará para almacenar la base de datos del Servidor de administración:

- **Microsoft SQL Server o SQL Server Express**
- **MySQL o MariaDB**
- **PostgreSQL o Postgres Pro**

Se recomienda instalar el Servidor de administración en un servidor dedicado y no en un controlador de dominio. Sin embargo, si instala Kaspersky Security Center en un servidor que actúe como controlador de dominio de solo lectura (RODC), Microsoft SQL Server (SQL Express) no se debe instalar de manera local (en el mismo dispositivo). En este caso, le recomendamos que instale Microsoft SQL Server (SQL Express) de forma remota (en un dispositivo diferente) o que use MySQL, MariaDB o PostgreSQL si necesita instalar el DBMS de manera local.

La estructura de la base de datos del Servidor de administración se proporciona en el archivo klakdb.chm, que se encuentra en la carpeta de instalación de Kaspersky Security Center. Este archivo también está disponible en un archivo en el portal de Kaspersky: klakdb.zip.

# Paso 7. Configurar el Servidor SQL

En este paso del asistente, especifique la siguiente configuración de conexión, según el sistema de administración de bases de datos (DBMS) que haya seleccionado:

- Si seleccionó **Microsoft SQL Server o SQL Server Express** en el paso anterior:

  - En el campo **Instancia de SQL Server**, especifique el nombre de SQL Server en la red. Para ver una lista de todas las instancias de SQL Server que estén en la red, haga clic en el botón **Examinar**. Este campo aparece en blanco de forma predeterminada.

    Si utiliza un puerto distinto del estándar para conectarse a SQL Server, indique el número de puerto junto con el nombre del host de SQL Server, separando los dos datos con una coma. Por ejemplo:

    ```
    nombre_host_SQL_Server, 1433
    ```

    Si utiliza un certificado para proteger las comunicaciones entre el Servidor de administración y SQL Server, asegúrese de que el nombre de host que escriba en el campo **Instancia de SQL Server** sea el mismo que haya utilizado para generar el certificado. Si utiliza una instancia con nombre de SQL Server, junto con el nombre del host de SQL Server, especifique el número del puerto separado con una coma, por ejemplo:

    ```
    nombre_SQL_Server, 1433
    ```

    Si usa varias instancias de SQL Server en el mismo host, especifique además el nombre de la instancia separado con una barra diagonal inversa, por ejemplo:

    ```
    nombre_SQL_Server\nombre_instancia_SQL_Server, 1433
    ```

    Si un SQL Server en la red empresarial tiene habilitada la característica Always On, especifique el nombre del oyente del grupo de disponibilidad en el campo **Instancia de SQL Server**. Tenga en cuenta que el Servidor de administración solo admite el modo de disponibilidad de confirmación sincrónica cuando la característica Always On está habilitada.

  - En el campo **Nombre de la base de datos**, especifique el nombre de la base de datos que se creará para almacenar los datos del Servidor de administración. El valor predeterminado es *KAV*.

  Si en esta etapa desea instalar SQL Server en el dispositivo desde el cual está instalando Kaspersky Security Center, debe detener la instalación y reiniciarla después de la instalación de SQL Server. Las versiones compatibles de SQL Server figuran en los requisitos del sistema.

  Si está instalando SQL Server en un dispositivo remoto, no es preciso interrumpir el asistente de instalación de Kaspersky Security Center. Instale el servidor SQL Server y luego continúe con la instalación de Kaspersky Security Center.

- Si seleccionó **MySQL o MariaDB** en el paso anterior:

  - En el campo **Instancia de SQL Server**, especifique el nombres de la instancia de DBMS. De forma predeterminada, el nombre es la dirección IP del dispositivo en el cual se debe instalar Kaspersky Security Center.

  - En el campo **Puerto**, especifique el puerto para la conexión del Servidor de administración con el DBMS. El número de puerto predeterminado es 3306.

  - En el campo **Nombre de la base de datos**, especifique el nombre de la base de datos que se creará para almacenar los datos del Servidor de administración. El valor predeterminado es *KAV*.

- Si seleccionó **PostgreSQL o Postgres Pro** en el paso anterior:

- En el campo **Servidor PostgreSQL o Postgres Pro**, especifique el nombre de la instancia de DBMS. De forma predeterminada, el nombre es la dirección IP del dispositivo en el cual se debe instalar Kaspersky Security Center.

- En el campo **Puerto**, especifique el puerto para la conexión del Servidor de administración con el DBMS. El número de puerto predeterminado es 5432.

- En el campo **Nombre de la base de datos**, especifique el nombre de la base de datos que se creará para almacenar los datos del Servidor de administración. El valor predeterminado es *KAV*.

## Paso 8. Seleccionar el modo de autenticación

Determine el modo de autenticación que se utilizará cuando el Servidor de administración se conecte con el sistema de administración de bases de datos (DBMS).

Según el DBMS seleccionado, puede elegir entre los siguientes modos de autenticación:

- Para el servidor SQL Express o Microsoft SQL Server, seleccione una de las siguientes opciones:

  - **Modo de autenticación de Microsoft Windows**. La verificación de permisos usa la cuenta utilizada para el inicio del Servidor de administración.

  - **Modo de autenticación de SQL Server**. Si selecciona esta opción, la cuenta especificada en la ventana se usa para verificar los permisos de acceso. Rellene los campos **Cuenta** y **Contraseña**.

    Para ver la contraseña introducida, haga clic y mantenga presionado el botón **Mostrar**.

  Para ambos modos de autenticación, la aplicación comprueba si la base de datos está disponible. Si la base de datos no está disponible, se muestra un mensaje de error y debe proporcionar las credenciales correctas.

  Si la base de datos del Servidor de administración se almacena en otro dispositivo y la cuenta del Servidor de administración no tiene el acceso al servidor de la base de datos, debe usar el modo de autenticación de SQL Server al instalar o actualizar el Servidor de administración. Esto puede ocurrir cuando el dispositivo que almacena la base de datos se encuentra fuera del dominio o cuando el Servidor de administración está instalado en la cuenta LocalSystem.

- Para MySQL, MariaDB, PostgreSQL o Postgres Pro, especifique la cuenta y la contraseña.

# Paso 9. Seleccionar la cuenta para iniciar el Servidor de administración

Seleccione la cuenta que será usada para iniciar el Servidor de administración como un servicio.

- **Generar automáticamente la cuenta**. La aplicación crea una cuenta llamada KL-AK-* en la que se ejecutará el servicio kladminserver.

  Puede seleccionar esta opción si planea localizar la carpeta compartida y el DBMS en el mismo dispositivo que el Servidor de administración.

- **Seleccione una cuenta**. El servicio del Servidor de administración (kladminserver) se ejecutará en la cuenta que seleccionó.

  Tendrá que seleccionar una cuenta de dominio si, por ejemplo, planea usar como DBMS una instancia de SQL Server de alguna versión, incluido SQL Express, que se encuentra en otro dispositivo o está planeando localizar la carpeta compartida en otro dispositivo.

  Kaspersky Security Center es compatible con cuentas de servicios administrados (MSA) y cuentas de servicios administrados en grupo (gMSA). Si se utilizan estos tipos de cuentas en su dominio, puede seleccionar una de ellas como la cuenta para el servicio del Servidor de administración.

  Antes de especificar las MSA o las gMSA, debe instalar la cuenta en el mismo dispositivo en el que desea instalar el Servidor de administración. Si la cuenta aún no está instalada, cancele la instalación del Servidor de administración, instale la cuenta y, luego, reinicie la instalación del Servidor de administración. Para obtener más información sobre la instalación de cuentas de servicio administradas en un dispositivo local, consulte la documentación oficial de Microsoft.

  *Para especificar las MSA o las gMSA:*

  1. Haga clic en el botón **Examinar**.
  2. En la ventana que se abre, haga clic en el botón **Tipo de objeto**.
  3. Seleccione **Cuenta para servicios** escriba y haga clic en **Aceptar**.
  4. Seleccione la cuenta relevante y haga clic en **Aceptar**.

La cuenta que seleccionó debe tener permisos diferentes, según qué DBMS planea usar.

Por razones de seguridad, no asigne el estado privilegiado a la cuenta en la cual ejecuta el Servidor de administración.

La cuenta del Servidor de administración no se puede cambiar posteriormente. Debe reinstalar el clúster de conmutación por error para utilizar otra cuenta del Servidor de administración.

## Paso 10. Selección de una cuenta para ejecutar los servicios de Kaspersky Security Center

Seleccione la cuenta a través de la cual los servicios de Kaspersky Security Center se ejecutarán en este dispositivo:

- **Generar automáticamente la cuenta**. Kaspersky Security Center crea una cuenta local denominada KlScSvc en este dispositivo en el grupo kladmins. Los servicios de Kaspersky Security Center se ejecutarán con la cuenta que se ha creado.

- **Seleccione una cuenta**. Los servicios de Kaspersky Security Center se ejecutarán en la cuenta que seleccionó.

  Deberá seleccionar una cuenta de dominio si, por ejemplo, tiene la intención de guardar informes a una carpeta ubicada en un dispositivo diferente o si esto es un requisito de la directiva de seguridad de su organización. También es posible que deba seleccionar una cuenta de dominio si instala el Servidor de administración en un clúster de conmutación por error.

Por razones de seguridad, no conceda estado privilegiado a la cuenta en la cual se ejecutan los servicios.

El servicio del proxy de KSN (ksnproxy), el servicio de proxy de activación de Kaspersky (klactprx) y el servicio del portal de autenticación de Kaspersky (klwebsrv) se ejecutarán en la cuenta seleccionada.

## Paso 11. Seleccionar una carpeta compartida

Defina la ubicación y el nombre de la carpeta compartida que se usará para realizar lo siguiente:

- Almacenar los archivos necesarios para la instalación remota de aplicaciones (los archivos se copian al Servidor de administración durante la creación de los paquetes de instalación).

- Almacenar actualizaciones que se han descargado de un origen de actualizaciones al Servidor de administración.

El uso compartido de archivos (solo lectura) estará habilitado para todos los usuarios.

Puede seleccionar cualquiera de las siguientes opciones:

- **Crear una carpeta compartida**. Crear una nueva carpeta. En el cuadro de texto, especifique la ruta a la carpeta.

- **Seleccionar una carpeta compartida existente**. Seleccione una carpeta compartida que ya exista.

La carpeta compartida puede ser una carpeta local en el dispositivo usado para la instalación o un directorio remoto en cualquier dispositivo cliente dentro de la red corporativa. Se puede usar el botón **Examinar** para seleccionar la carpeta compartida o especificarla de forma manual al ingresar la ruta UNC (por ejemplo, \\server\Share) en el campo correspondiente.

De manera predeterminada, el instalador crea una subcarpeta KLSHARE local en la carpeta de la aplicación que contiene los componentes de Kaspersky Security Center.

Puede definir una carpeta compartida posteriormente si es necesario.

# Paso 12. Configurar la conexión al Servidor de administración

Configurar la conexión con el Servidor de administración:

- **Puerto**

  El número de puerto utilizado para conectar con el Servidor de administración.

  El número de puerto predeterminado es 14000.

- **Puerto SSL**

  El número de puerto SSL (Capa de sockets seguros) se usa para conectarse de manera segura al Servidor de administración mediante SSL.

  El número de puerto predeterminado es 13000.

- **Longitud de la clave de cifrado**

  Seleccione la longitud de la clave de cifrado: 1024 bits o 2048 bits.

  Una clave de cifrado de 1024 bits aplica una carga más pequeña en la CPU, pero se considera obsoleta porque no puede proporcionar cifrado confiable debido a sus especificaciones técnicas. Además, el hardware existente probablemente resultará incompatible con certificados de SSL que presentan claves de 1024 bits.

  Una clave de cifrado de 2048 bits cumple todos los estándares del cifrado de última generación. Sin embargo, el uso de una clave de cifrado de 2048 bits puede aumentar la carga en la CPU.

  Por defecto, **2048 bits (mayor seguridad)** está seleccionado.

También puede cambiar los parámetros para conectarse al Servidor de administración más adelante de la siguiente manera:

- Puede cambiar el puerto y los números de puerto SSL en la sección **Puertos de conexión** de las propiedades del Servidor de administración. Para obtener más información sobre los puertos de conexión del Servidor de administración, consulte Puertos utilizados por Kaspersky Security Center.

- Puede cambiar la longitud de la clave de cifrado cuando reemplaza el certificado del Servidor de administración con la utilidad klsetsrvcert mediante el parámetro `-o RsaKeyLen:<longitud de la clave>`.

## Paso 13. Definir la dirección del Servidor de administración

Especifique la dirección del Servidor de administración mediante uno de los siguientes métodos:

- **Nombre de dominio DNS**. Puede utilizar este método si la red incluye un servidor DNS y los dispositivos cliente pueden utilizarlo para recibir la dirección del Servidor de administración.
- **Nombre NetBIOS**. Puede utilizar este método si los dispositivos cliente reciben la dirección del Servidor de administración mediante el protocolo NetBIOS o si hay un servidor WINS disponible en la red.
- **Dirección IP**. Puede utilizar este método si el Servidor de administración tiene una dirección IP estática que no se modificará posteriormente.

Si instala Kaspersky Security Center en el nodo activo del clúster de conmutación por error de Kaspersky Security Center y creó un adaptador de red virtual al preparar los nodos del clúster, especifique la dirección IP de este adaptador. De lo contrario, ingrese la dirección IP del equilibrador de carga de terceros que utiliza.

## Paso 14. Dirección del Servidor de administración para la conexión de dispositivos móviles

Este paso del asistente de instalación se encuentra disponible si ha seleccionado la Administración de dispositivos móviles para la instalación.

En la ventana **Dirección para la conexión de dispositivos móviles**, especifique la dirección externa del Servidor de administración para la conexión de los dispositivos móviles que están fuera de la red local. Puede especificar la dirección IP o el Sistema de nombres de dominio (DNS) del Servidor de administración.

## Paso 15. Seleccionar complementos de administración de aplicaciones

Seleccione los complementos de administración de aplicaciones que deben instalarse con Kaspersky Security Center.

Para facilitar la búsqueda, los complementos se dividen en grupos según el tipo de objetos asegurados.

## Paso 16. Desempaquetar e instalar archivos en el disco duro

Después de configurar la instalación de los componentes de Kaspersky Security Center, puede comenzar con la instalación de archivos en el disco duro.

Si la instalación requiere programas adicionales, el asistente de instalación se lo notificará en la página **Instalando requisitos previos** antes de instalar Kaspersky Security Center. Los programas requeridos se instalarán automáticamente después de hacer clic en el botón **Siguiente**.

En la última página, puede seleccionar qué consola desea iniciar para trabajar con Kaspersky Security Center:

- **Iniciar Consola de administración basada en MMC**
- **Iniciar Kaspersky Security Center Web Console**

  Esta opción solo está disponible si ha optado por instalar Kaspersky Security Center Web Console en uno de los pasos anteriores.

También puede hacer clic en **Finalizar** para cerrar el asistente sin comenzar a trabajar con Kaspersky Security Center. Puede iniciar el trabajo más tarde en cualquier momento.

Al iniciar por primera vez la Consola de administración o Kaspersky Security Center Web Console, puede realizar la configuración inicial de la aplicación.

# Despliegue del clúster de conmutación por error de Kaspersky Security Center

Esta sección contiene información general sobre el clúster de conmutación por error de Kaspersky Security Center e instrucciones sobre la preparación y el despliegue del clúster de conmutación por error de Kaspersky Security Center en su red.

## Escenario: Despliegue de un clúster de conmutación por error de Kaspersky Security Center

Un clúster de conmutación por error de Kaspersky Security Center proporciona una alta disponibilidad de Kaspersky Security Center y minimiza el tiempo de inactividad del Servidor de administración en caso de una falla. El clúster de conmutación por error se basa en dos instancias idénticas de Kaspersky Security Center instaladas en dos equipos. Una de las instancias funciona como nodo activo y la otra como nodo pasivo. El nodo activo administra la protección de los dispositivos cliente, mientras que el pasivo está preparado para asumir todas las funciones del nodo activo en caso de que falle el nodo activo. Cuando ocurre una falla, el nodo pasivo se activa y el nodo activo se vuelve pasivo.

### Requisitos previos

Cuenta con hardware que cumple con los requisitos para el clúster de conmutación por error.

### Etapas

El despliegue de las aplicaciones de Kaspersky se divide en etapas:

1. **Crear una cuenta para los servicios de Kaspersky Security Center**

   Cree un nuevo grupo de dominio (en este escenario, se utiliza el nombre "KLAdmins" para este grupo) y conceda los permisos de administrador local al grupo en ambos nodos y en el servidor de archivos. A continuación, cree dos nuevas cuentas de usuario de dominio (en este escenario, se usan los nombres "ksc" y "rightless" para estas cuentas) y agregue las cuentas al grupo de dominio KLAdmins.

   Agregue la cuenta de usuario, en la cual se instalará Kaspersky Security Center, al grupo de dominio KLAdmins creado anteriormente.

2. **Preparación del servidor de archivos**

   Prepare el servidor de archivos para que funcione como un componente del clúster de conmutación por error de Kaspersky Security Center. Asegúrese de que el servidor de archivos cumpla con los requisitos de hardware y software, cree dos carpetas compartidas para los datos de Kaspersky Security Center y configure los permisos para acceder a las carpetas compartidas.

   Instrucciones: Preparación de un servidor de archivos para el clúster de conmutación por error de Kaspersky Security Center

3. **Preparación de nodos activos y pasivos**

   Prepare dos dispositivos con hardware y software idénticos para que funcionen como el nodo activo y pasivo.

   Instrucciones: Preparación de nodos para el clúster de conmutación por error de Kaspersky Security Center

4. **Instalación del sistema de administración de bases de datos (DBMS)**

   Seleccione cualquiera de los DBMS compatibles y, luego, instale el DBMS en un dispositivo dedicado. Para obtener información sobre cómo instalar el DBMS, consulte la documentación.

5. **Instalación de Kaspersky Security Center**

   Instale Kaspersky Security Center en el modo de clúster de conmutación por error en ambos nodos. Primero debe instalar Kaspersky Security Center en el dispositivo que desee que sea el host activo y luego en el pasivo.

   Debe instalar Kaspersky Security Center Web Console en un dispositivo independiente que no sea un nodo del clúster.

   Instrucciones: Instalación de Kaspersky Security Center en los nodos del clúster de conmutación por error de Kaspersky Security Center

6. **Prueba del clúster de conmutación por error**

   Compruebe que haya configurado correctamente el clúster de conmutación por error y que funcione correctamente. Por ejemplo, puede detener uno de los servicios de Kaspersky Security Center en el nodo activo: kladminserver, klnagent, ksnproxy, klactprx o klwebsrv. Una vez que se detiene el servicio, la administración de la protección se debe cambiar automáticamente al nodo pasivo.

### Resultados

El clúster de conmutación por error de Kaspersky Security Center se encuentra desplegado. Familiarícese con los eventos que conducen al cambio entre los nodos activo y pasivo.

## Sobre el clúster de conmutación por error de Kaspersky Security Center

Un clúster de conmutación por error de Kaspersky Security Center proporciona una alta disponibilidad de Kaspersky Security Center y minimiza el tiempo de inactividad del Servidor de administración en caso de una falla. El clúster de conmutación por error se basa en dos instancias idénticas de Kaspersky Security Center instaladas en dos equipos. Una de las instancias funciona como nodo activo y la otra como nodo pasivo. El nodo activo administra la protección de los dispositivos cliente, mientras que el pasivo está preparado para asumir todas las funciones del nodo activo en caso de que falle el nodo activo. Cuando ocurre una falla, el nodo pasivo se activa y el nodo activo se vuelve pasivo.

El uso del clúster de conmutación por error no afecta los cálculos basados en la guía de dimensionamiento.

Utilice la función registro de eventos de Kaspersky para solucionar problemas.

## Condiciones para el cambio

El clúster de conmutación por error cambia la administración de protección de los dispositivos cliente del nodo activo al nodo pasivo si ocurre alguno de los siguientes eventos en el nodo activo:

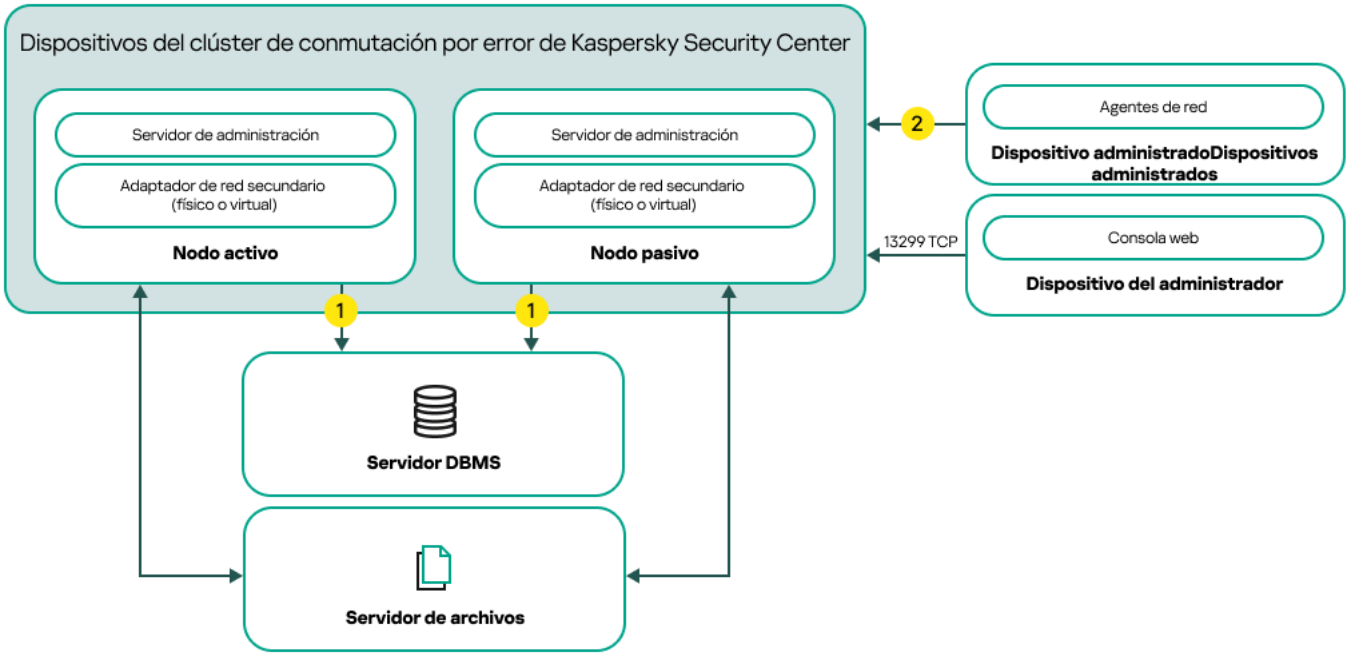
- El nodo activo se rompe debido a una falla de software o hardware.
- El nodo activo se detiene temporalmente por actividades de mantenimiento.
- Al menos uno de los servicios (o procesos) de Kaspersky Security Center falla o se cancela deliberadamente por el usuario. Los servicios de Kaspersky Security Center son los siguientes: kladminserver, klnagent, klactprx y klwebsrv.
- La conexión de red entre el nodo activo y el almacenamiento en el servidor de archivos se interrumpe o termina.

El clúster de conmutación por error de Kaspersky Security Center administra todos los servicios de Kaspersky Security Center automáticamente. No reinicie los servicios de forma manual.

## Esquemas de despliegue

Puede elegir uno de los siguientes esquemas para desplegar el clúster de conmutación por error de Kaspersky Security Center:

- Un esquema que utiliza un adaptador de red secundario.
- Un esquema que utiliza un equilibrador de carga externo.

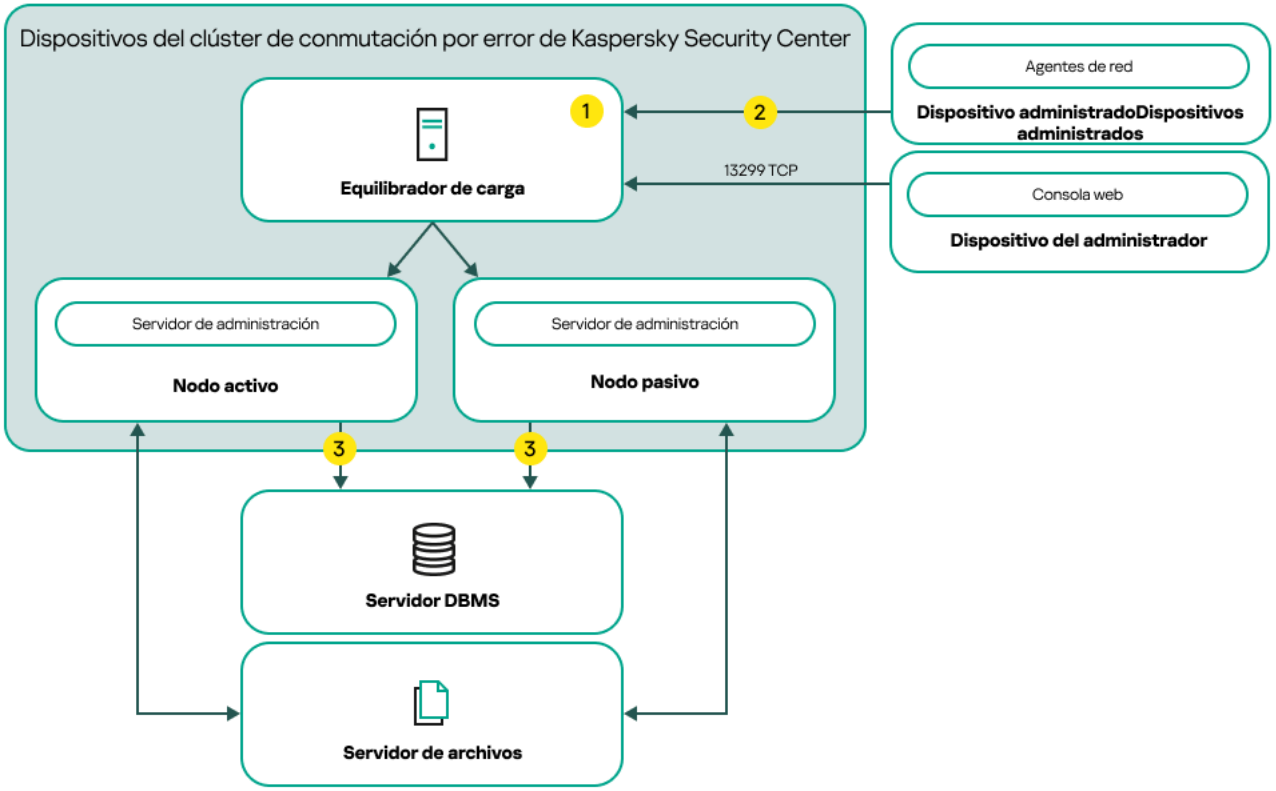



Un esquema que usa un adaptador de red secundario

Leyenda del esquema:

1 El Servidor de administración envía información a la base de datos. Abra los puertos necesarios en el dispositivo donde se encuentra la base de datos, por ejemplo, el puerto 3306 para MySQL Server o el puerto 1433 para Microsoft SQL Server. Consulte la documentación del DBMS para obtener la información necesaria.

2 En los dispositivos administrados, abra los siguientes puertos: TCP 13000, UDP 13000 y TCP 17000.




Un esquema que utiliza un equilibrador de carga externo

Leyenda del esquema:

1 En el dispositivo equilibrador de carga, abra todos los puertos del Servidor de administración: TCP 13000, UDP 13000, TCP 13299 y TCP 17000.

> Si desea usar la utilidad klakaut para la automatización, también debe abrir el puerto TCP 13291.

2 En los dispositivos administrados, abra los siguientes puertos: TCP 13000, UDP 13000 y TCP 17000.

3 El Servidor de administración envía información a la base de datos. Abra los puertos necesarios en el dispositivo donde se encuentra la base de datos, por ejemplo, el puerto 3306 para MySQL Server o el puerto 1433 para Microsoft SQL Server. Consulte la documentación del DBMS para obtener la información necesaria.

## Preparación de un servidor de archivos para un clúster de conmutación por error de Kaspersky Security Center

Un servidor de archivos funciona como un componente necesario en un clúster de conmutación por error de Kaspersky Security Center.

*Para preparar un servidor de archivos, haga lo siguiente:*

1. Asegúrese de que el servidor de archivos cumpla con los requisitos de hardware y software.
2. Asegúrese de que el servidor de archivos y ambos nodos (activo y pasivo) estén incluidos en el mismo dominio o que el servidor de archivos sea el controlador de dominio.

3. En el servidor de archivos, cree dos carpetas compartidas. Una de ellas se utiliza para almacenar información sobre el estado del clúster de conmutación por error. La otra se utiliza para almacenar los datos y la configuración de Kaspersky Security Center. Deberá especificar las rutas a las carpetas compartidas mientras configura la instalación de Kaspersky Security Center.

4. Otorgue permisos de acceso completo (tanto permisos compartidos como permisos NTFS) a las carpetas compartidas creadas para los siguientes grupos y cuentas de usuario:

   - Grupo de dominio KLAdmins.
   - Cuentas de usuario $<node1> y $<node2>. Aquí, <node1> y <node2> son los nombres de dispositivo de los nodos activos y pasivos.

El servidor de archivos está preparado. Para desplegar el clúster de conmutación por error de Kaspersky Security Center, siga las instrucciones adicionales en este escenario.

## Preparación de nodos para un clúster de conmutación por error de Kaspersky Security Center

Prepare dos dispositivos para que funcionen como los nodos activo y pasivo del clúster de conmutación por error de Kaspersky Security Center.

*Para preparar nodos para un clúster de conmutación por error de Kaspersky Security Center, haga lo siguiente:*

1. Asegúrese de tener dos dispositivos que cumplen los requisitos de hardware y software. Estos dispositivos actuarán como nodos activos y pasivos del clúster de conmutación por error.

2. Asegúrese de que el servidor de archivos y ambos nodos estén incluidos en el mismo dominio.

3. Realice una de las siguientes acciones:

   - Configure un adaptador de red secundario en cada uno de los nodos.

     Un adaptador de red secundario puede ser físico o virtual. Si desea utilizar un adaptador de red físico, conéctelo y configúrelo con herramientas estándar del sistema operativo. Si desea utilizar un adaptador de red virtual, créelo con un software de terceros.

     Asegúrese de que se cumplan las siguientes condiciones:

     - Los adaptadores de red secundarios están deshabilitados.

       Puede crear los adaptadores de red virtuales en el estado deshabilitado o deshabilitarlos después de la creación.

     - Los adaptadores de red secundarios en ambos nodos deben tener la misma dirección IP.

   - Utilice un equilibrador de carga de terceros. Por ejemplo, puede utilizar un servidor nginx. En este caso, haga lo siguiente:

     a. Proporcione un dispositivo dedicado basado en Linux con nginx instalado.

     b. Configure el equilibrio de carga. Configure el nodo activo como servidor principal y el nodo pasivo como servidor de respaldo.

     c. En el servidor nginx, abra todos los puertos del Servidor de administración: TCP 13000, UDP 13000, TCP 13299 y TCP 17000.

        Si desea usar la utilidad klakaut para la automatización, también debe abrir el puerto TCP 13291.

4. Reinicie ambos nodos y el servidor de archivos.

5. Asigne las dos carpetas compartidas que creó durante el paso de preparación del servidor de archivos a cada uno de los nodos. Debe asignar las carpetas compartidas como unidades de red. Al asignar las carpetas, puede seleccionar cualquier letra de unidad vacante. Para acceder a las carpetas compartidas, use las credenciales de la cuenta de usuario que creó durante el paso 1 del escenario.

Los nodos están preparados. Para desplegar el clúster de conmutación por error de Kaspersky Security Center, siga las instrucciones adicionales del escenario.

## Instalación de Kaspersky Security Center en los nodos del clúster de conmutación por error de Kaspersky Security Center

Kaspersky Security Center se instala por separado en ambos nodos del clúster de conmutación por error de Kaspersky Security Center. Primero, debe instalar la aplicación en el nodo activo, luego en el pasivo. Durante la instalación, elija qué nodo estará activo y cuál será pasivo.

Solo un usuario del grupo de dominio KLAdmins puede instalar Kaspersky Security Center en cada nodo.

*Para instalar Kaspersky Security Center en el nodo activo del clúster de conmutación por error de Kaspersky Security Center, haga lo siguiente:*

1. Ejecute el archivo ejecutable ksc_15.1_ <número de compilación> _full_ <idioma> .exe.

   Se abre una ventana y se le solicita que seleccione las aplicaciones de Kaspersky que desea instalar. En la ventana de selección de aplicaciones, haga clic en el vínculo **Instalar el Servidor de administración de Kaspersky Security Center** para que se inicie el Asistente de instalación del Servidor de administración. Siga las instrucciones del asistente.

2. Por favor lea con atención el Contrato de licencia y la Política de privacidad. Si está de acuerdo con todos los términos del Contrato de licencia y la Política de privacidad, seleccione las casillas siguientes en la sección **Confirmo que he leído y comprendido la totalidad del texto, y que acepto lo siguiente**:

   - **Los términos y las condiciones de este EULA**
   - **la Política de privacidad que describe el manejo de los datos**

   La instalación de la aplicación en su dispositivo continuará después de que seleccione ambas casillas.

   Si no acepta el Contrato de licencia o la Política de privacidad, cancele la instalación haciendo clic en el botón **Cancelar**.

3. Seleccione **Nodo principal del clúster de conmutación por error de Kaspersky Security Center** para instalar la aplicación en el nodo activo.

4. En la ventana **Carpeta compartida**, haga lo siguiente:

   - En los campos **Estado compartido** y **Datos compartidos**, especifique las rutas a las carpetas compartidas que creó en el servidor de archivos durante la preparación.
   - En los campos **Unidad de estado compartido** y **Unidad de datos compartidos**, seleccione las unidades de red a las que asignó las carpetas compartidas durante la preparación de los nodos.
   - Seleccione el modo de conectividad del clúster: a través de un adaptador de red secundario o un equilibrador de carga de terceros.

5. Realice otros pasos de instalación personalizada, comenzando con paso 3.

   > En el paso 13, especifique la dirección IP de un adaptador de red virtual si creó un adaptador al preparar los nodos del clúster. De lo contrario, ingrese la dirección IP del equilibrador de carga de terceros que utiliza.

Kaspersky Security Center está instalado en el nodo activo.

*Para instalar Kaspersky Security Center en el nodo pasivo del clúster de conmutación por error de Kaspersky Security Center, haga lo siguiente:*

1. Ejecute el archivo ejecutable ksc_15.1_ <número de compilación> _full_ <idioma> .exe.

   Se abre una ventana y se le solicita que seleccione las aplicaciones de Kaspersky que desea instalar. En la ventana de selección de aplicaciones, haga clic en el vínculo **Instalar el Servidor de administración de Kaspersky Security Center** para que se inicie el Asistente de instalación del Servidor de administración. Siga las instrucciones del asistente.

2. Por favor lea con atención el Contrato de licencia y la Política de privacidad. Si está de acuerdo con todos los términos del Contrato de licencia y la Política de privacidad, seleccione las casillas siguientes en la sección **Confirmo que he leído y comprendido la totalidad del texto, y que acepto lo siguiente**:

   - **Los términos y las condiciones de este EULA**
   - **la Política de privacidad que describe el manejo de los datos**

   La instalación de la aplicación en su dispositivo continuará después de que seleccione ambas casillas.

   Si no acepta el Contrato de licencia o la Política de privacidad, cancele la instalación haciendo clic en el botón **Cancelar**.

3. Seleccione **Nodo secundario del clúster de conmutación por error de Kaspersky Security Center** para instalar la aplicación en el nodo pasivo.

4. En la ventana **Carpeta compartida**, en el campo **Estado compartido**, especifique una ruta a la carpeta compartida con información sobre el estado del clúster que creó en el servidor de archivos durante la preparación.

5. Haga clic en el botón **Instalar**. Cuando finalice la instalación, haga clic en el botón **Finalizar**.

Kaspersky Security Center está instalado en el nodo pasivo. Ahora, puede probar el clúster de conmutación por error de Kaspersky Security Center para asegurarse de que lo configuró de forma correcta y de que funciona bien.

## Iniciar y detener nodos del clúster manualmente

Es posible que deba detener todo el clúster de conmutación por error de Kaspersky Security Center o desconectar de forma temporal uno de los nodos del clúster para realizar tareas de mantenimiento. Si este es el caso, siga las instrucciones de esta sección. No intente iniciar ni detener los servicios o procesos relacionados con el clúster de conmutación por error utilizando ningún otro medio. Esto puede provocar la pérdida de datos.

### Iniciar y detener todo el clúster de conmutación por error para mantenimiento

*Para iniciar o detener todo el clúster de conmutación por error, haga lo siguiente:*

1. En el nodo activo, vaya a <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Abra la línea de comando y luego ejecute uno de los siguientes comandos:

   - Para detener el clúster, ejecute: `klfoc -stopcluster --stp klfoc`
   - Para iniciar el clúster, ejecute: `klfoc -startcluster --stp klfoc`

El clúster de conmutación por error se inicia o se detiene según el comando que ejecute.

### Mantenimiento de uno de los nodos

*Para mantener uno de los nodos, haga lo siguiente:*

1. En el nodo activo, detenga el clúster de conmutación por error mediante el comando `klfoc -stopcluster --stp klfoc`.
2. En el nodo que desea mantener, vaya a <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
3. Abra la línea de comandos y, luego, desconecte el nodo del clúster mediante la ejecución del comando `detach_node.cmd`.
4. En el nodo activo, inicie el clúster de conmutación por error mediante el comando `klfoc -startcluster --stp klfoc`.
5. Realizar actividades de mantenimiento.
6. En el nodo activo, detenga el clúster de conmutación por error mediante el comando `klfoc -stopcluster --stp klfoc`.
7. En el nodo que se mantuvo, vaya a <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
8. Abra la línea de comandos y, luego, conecte el nodo al clúster mediante la ejecución del comando `attach_node.cmd`.
9. En el nodo activo, inicie el clúster de conmutación por error mediante el comando `klfoc -startcluster --stp klfoc`.

El nodo se mantiene y se adjunta al clúster de conmutación por error.

## Instalación del Servidor de administración en un clúster de conmutación por error de Windows Server

El procedimiento para instalar el Servidor de administración en un clúster de conmutación por error difiere de la instalación estándar y personalizada que se realiza en un dispositivo independiente.

Aplique el procedimiento que se describe en esta sección al nodo que contiene un almacenamiento de datos común del clúster.

*Para instalar el Servidor de administración de Kaspersky Security Center en un dispositivo local, realice lo siguiente:*

Ejecute el archivo ejecutable ksc_<número de versión>.<número de compilación>_full_<idioma de localización>.exe.

Se abre una ventana y se le solicita que seleccione las aplicaciones de Kaspersky que desea instalar. En la ventana de selección de aplicaciones, haga clic en el enlace **Instalar del Servidor de administración de Kaspersky Security Center** para ejecutar el asistente de instalación del Servidor de administración. Siga las instrucciones del asistente.

## Paso 1. Revisar el Contrato de licencia y la Política de privacidad

En esta etapa del Asistente de instalación, debe leer el Contrato de licencia, que se establecerá entre usted y Kaspersky, así como la Política de privacidad.

También se le puede solicitar que vea los Contratos de licencia y las Políticas de privacidad para los complementos de administración de aplicaciones que están disponibles en el kit de distribución de Kaspersky Security Center.

Por favor lea con atención el Contrato de licencia y la Política de privacidad. Si está de acuerdo con todos los términos del Contrato de licencia y la Política de privacidad, confírmelo seleccionando las casillas de verificación correspondientes.

La instalación de la aplicación en su dispositivo continuará después de que seleccione ambas casillas.

Si no acepta el Contrato de licencia o la Política de privacidad, cancele la instalación haciendo clic en el botón **Cancelar**.

## Paso 2. Seleccionar el tipo de instalación en un clúster

Seleccione el tipo de instalación en el clúster:

- **Clúster (instalar en todos los nodos del clúster)**

  Esta es la opción recomendada. Si selecciona esta opción, el Servidor de administración se instalará en todos los nodos del clúster de forma simultánea.

  > En el paso de selección de la Consola de administración para la instalación, deberá seleccionar la consola que se instalará en el nodo del clúster actual. Si instala una consola únicamente en el nodo del clúster y dicho nodo sufre un problema de funcionamiento, quedará sin acceso al Servidor de administración. Le recomendamos que durante este paso, seleccione la Consola de administración basada en MMC para la instalación en todos los nodos del clúster. Después de instalar el Servidor de administración, instale Kaspersky Security Center Web Console en un dispositivo independiente que no sea un nodo del clúster. Esto le permite administrar el Servidor de administración mediante Kaspersky Security Center Web Console si falla el nodo del clúster.

- **Local (instalar solamente en este dispositivo)**

  Si selecciona esta opción, el Servidor de administración se instalará solo en el nodo actual, como si fuera un servidor independiente, y el Servidor de administración no funcionará como una aplicación compatible con clústeres. Por ejemplo, es posible que desee elegir esta opción para ahorrar espacio de almacenamiento compartido si no se necesita la tolerancia a errores en el Servidor de administración. En caso de que se produzca un error en el nodo actual, deberá instalar el Servidor de administración en otro nodo y restaurar el estado del Servidor de administración desde una copia de seguridad.

Los pasos siguientes son los mismos que cuando utiliza el método de instalación estándar o personalizado, desde el paso de selección del método de instalación.

## Paso 3. Especificar el nombre del Servidor de administración virtual

Especifique el nombre de la red del nuevo Servidor de administración virtual. Podrá utilizar este nombre para conectar la Consola de administración o Kaspersky Security Center Web Console al Servidor de administración.

El nombre que especifique no debe ser igual que el nombre del clúster.

## Paso 4. Especificar los datos de la red del Servidor de administración virtual

*Para especificar los datos de la red de la nueva instancia del Servidor de administración virtual, realice lo siguiente:*

1. En **Red para utilizar**, seleccione la red de dominios a la que está conectado el nodo del clúster actual.
2. Realice una de las siguientes acciones:
   - Si se utiliza un DHCP en la red seleccionada para asignar direcciones IP, marque la opción **Utilizar DHCP**.
   - Si no se utiliza DHCP en la red seleccionada, especifique la dirección IP que necesite.

     La dirección IP que especifique no debe ser igual que la dirección IP del clúster.
3. Haga clic en **Agregar** para aplicar la configuración que especificó.

Podrá utilizar la dirección IP que se asignó automáticamente o la que especificó para conectar la Consola de administración o Kaspersky Security Center Web Console al Servidor de administración.

## Paso 5. Especificar un grupo de clústeres

Un grupo de clústeres constituye una función de clúster de conmutación por error especial que contiene recursos comunes para todos los nodos. Usted cuenta con dos opciones:

- Crear un grupo de clústeres nuevo.

  En la mayoría de los casos, esta es la opción recomendada. El grupo de clústeres nuevo contendrá todos los recursos comunes relacionados con la instancia del Servidor de administración.

- Seleccionar un grupo de clústeres existente.

  Seleccione esta opción si desea utilizar un recurso común que ya está asociado a un grupo de clústeres existente. Por ejemplo, es posible que desee utilizar esta opción si pretende utilizar un almacenamiento asociado con un grupo de clústeres existente y si no existe otro almacenamiento disponible para un grupo de clústeres nuevo.

## Paso 6. Seleccionar un almacenamiento de datos de clúster

*Para seleccionar un almacenamiento de datos de clúster, realice lo siguiente:*

1. En **Repositorios disponibles**, seleccione el almacenamiento de datos en el que se instalarán los recursos comunes de la instancia del Servidor de administración virtual.
2. Si el almacenamiento de datos seleccionado contiene varias cantidades, en **Secciones disponibles en la unidad de disco**, seleccione la cantidad que necesite.
3. En **Ruta de instalación**, ingrese la ruta del almacenamiento de datos común en la que se instalarán los recursos de la instancia del Servidor de administración virtual.

Así se selecciona el almacenamiento de datos.

## Paso 7. Especificar una cuenta para realizar la instalación remota

Especifique el nombre de usuario y la contraseña que se utilizarán para la instalación remota de la instancia del Servidor de administración virtual en un nodo pasivo del clúster.

La cuenta que especifique debe contar con privilegios administrativos en todos los nodos del clúster.

## Paso 8. Seleccionar los componentes a instalar

Seleccione los componentes del Servidor de administración de Kaspersky Security Center que desee instalar:

- **Administración de dispositivos móviles**. Seleccione esta casilla de verificación si debe crear paquetes de instalación para dispositivos móviles cuando se esté ejecutando el asistente de instalación de Kaspersky Security Center. También puede crear paquetes de instalación para dispositivos móviles manualmente, después de la instalación del Servidor de administración, utilizando las herramientas de la Consola de administración.
- **Agente SNMP**. Este componente recibe la información estadística para el Servidor de administración a través del protocolo SNMP. El componente solamente está disponible si la aplicación se instala en un dispositivo con SNMP instalado.

  Después de instalar Kaspersky Security Center, los archivos .mib requeridos para recibir estadísticas se ubicarán en la subcarpeta SNMP de la carpeta de instalación de la aplicación.

El Agente de red y la Consola de administración no se muestran en la lista de componentes. Estos componentes se instalan de manera automática y no se puede cancelar su instalación.

En este paso, debe especificar una carpeta para instalar los componentes del Servidor de administración. De manera predeterminada, los componentes se instalan en <Disco>:\Archivos de programa\Kaspersky Lab\Kaspersky Security Center. Si no existe la carpeta, se crea en forma automática durante la instalación. Es posible cambiar la carpeta de destino usando el botón **Examinar**.

## Paso 9. Seleccionar el tamaño de la red

Especifique la escala de la red en la cual instalará Kaspersky Security Center. Según el número de dispositivos en la red, el asistente configura la instalación y el aspecto de la interfaz de la aplicación para que coincidan.

La siguiente tabla enumera la configuración de instalación de la aplicación y la configuración de la apariencia de la interfaz que se ajustan basadas en varios tamaños de red.

Correspondencia de la configuración de instalación con el tamaño de red seleccionado

| Configuración | De 1 a 100 dispositivos administrados | De 101 a 1000 dispositivos administrados | De 1001 a 5000 dispositivos administrados | Más de 5000 dispositivos administrados |
|---|---|---|---|---|
| Mostrar con el nodo de los Servidores de administración secundarios y virtuales y todos los parámetros de configuración relacionados con estos servidores en el árbol de consola (solo disponible en la Consola de administración basada en MMC) | No disponible | No disponible | Disponible | Disponible |
| Mostrar con las secciones **Seguridad** en las ventanas de propiedades del Servidor de administración y grupos de administración (solo disponible en la Consola de administración basada en MMC) | No disponible | No disponible | Disponible | Disponible |
| Distribuir aleatoriamente el tiempo de inicio de la tarea de actualización en los dispositivos cliente | No disponible | Sobre un intervalo de 5 minutos | Sobre un intervalo de 10 minutos | Sobre un intervalo de 10 minutos |

Si conecta el Servidor de administración a un servidor de bases de datos MySQL 5.7 o SQL Express, recomendamos que no use la aplicación para administrar más de 10 000 dispositivos. Para el servidor de bases de datos MariaDB, el máximo recomendado es de 20000 dispositivos administrados.

## Paso 10. Seleccionar una base de datos

En este paso del asistente, seleccione uno de los siguientes sistemas de gestión de bases de datos (DBMS) que se utilizará para almacenar la base de datos del Servidor de administración:

- **Microsoft SQL Server o SQL Server Express**
- **MySQL o MariaDB**
- **PostgreSQL o Postgres Pro**

Se recomienda instalar el Servidor de administración en un servidor dedicado y no en un controlador de dominio. Sin embargo, si instala Kaspersky Security Center en un servidor que actúe como controlador de dominio de solo lectura (RODC), Microsoft SQL Server (SQL Express) no se debe instalar de manera local (en el mismo dispositivo). En este caso, le recomendamos que instale Microsoft SQL Server (SQL Express) de forma remota (en un dispositivo diferente) o que use MySQL, MariaDB o PostgreSQL si necesita instalar el DBMS de manera local.

La estructura de la base de datos del Servidor de administración se proporciona en el archivo klakdb.chm, que se encuentra en la carpeta de instalación de Kaspersky Security Center. Este archivo también está disponible en un archivo en el portal de Kaspersky: klakdb.zip.

# Paso 11. Configurar el Servidor SQL

En este paso del asistente, especifique la siguiente configuración de conexión, según el sistema de administración de bases de datos (DBMS) que haya seleccionado:

- Si seleccionó **Microsoft SQL Server o SQL Server Express** en el paso anterior:

  - En el campo **Instancia de SQL Server**, especifique el nombre de SQL Server en la red. Para ver una lista de todas las instancias de SQL Server que estén en la red, haga clic en el botón **Examinar**. Este campo aparece en blanco de forma predeterminada.

    Si utiliza un puerto distinto del estándar para conectarse a SQL Server, indique el número de puerto junto con el nombre del host de SQL Server, separando los dos datos con una coma. Por ejemplo:

    ```
    nombre_host_SQL_Server, 1433
    ```

    Si utiliza un certificado para proteger las comunicaciones entre el Servidor de administración y SQL Server, asegúrese de que el nombre de host que escriba en el campo **Instancia de SQL Server** sea el mismo que haya utilizado para generar el certificado. Si utiliza una instancia con nombre de SQL Server, junto con el nombre del host de SQL Server, especifique el número del puerto separado con una coma, por ejemplo:

    ```
    nombre_SQL_Server, 1433
    ```

    Si usa varias instancias de SQL Server en el mismo host, especifique además el nombre de la instancia separado con una barra diagonal inversa, por ejemplo:

    ```
    nombre_SQL_Server\nombre_instancia_SQL_Server, 1433
    ```

    Si un SQL Server en la red empresarial tiene habilitada la característica Always On, especifique el nombre del oyente del grupo de disponibilidad en el campo **Instancia de SQL Server**. Tenga en cuenta que el Servidor de administración solo admite el modo de disponibilidad de confirmación sincrónica cuando la característica Always On está habilitada.

  - En el campo **Nombre de la base de datos**, especifique el nombre de la base de datos que se creará para almacenar los datos del Servidor de administración. El valor predeterminado es *KAV*.

  Si en esta etapa desea instalar SQL Server en el dispositivo desde el cual está instalando Kaspersky Security Center, debe detener la instalación y reiniciarla después de la instalación de SQL Server. Las versiones compatibles de SQL Server figuran en los requisitos del sistema.

  Si está instalando SQL Server en un dispositivo remoto, no es preciso interrumpir el asistente de instalación de Kaspersky Security Center. Instale el servidor SQL Server y luego continúe con la instalación de Kaspersky Security Center.

- Si seleccionó **MySQL o MariaDB** en el paso anterior:

  - En el campo **Instancia de SQL Server**, especifique el nombres de la instancia de DBMS. De forma predeterminada, el nombre es la dirección IP del dispositivo en el cual se debe instalar Kaspersky Security Center.

  - En el campo **Puerto**, especifique el puerto para la conexión del Servidor de administración con el DBMS. El número de puerto predeterminado es 3306.

  - En el campo **Nombre de la base de datos**, especifique el nombre de la base de datos que se creará para almacenar los datos del Servidor de administración. El valor predeterminado es *KAV*.

- Si seleccionó **PostgreSQL o Postgres Pro** en el paso anterior:

- En el campo **Servidor PostgreSQL o Postgres Pro**, especifique el nombre de la instancia de DBMS. De forma predeterminada, el nombre es la dirección IP del dispositivo en el cual se debe instalar Kaspersky Security Center.

- En el campo **Puerto**, especifique el puerto para la conexión del Servidor de administración con el DBMS. El número de puerto predeterminado es 5432.

En el campo **Nombre de la base de datos**, especifique el nombre de la base de datos que se creará para almacenar los datos del Servidor de administración. El valor predeterminado es *KAV*.

## Paso 12. Seleccionar el modo de autenticación

Determine el modo de autenticación que se utilizará cuando el Servidor de administración se conecte con el sistema de administración de bases de datos (DBMS).

Según el DBMS seleccionado, puede elegir entre los siguientes modos de autenticación:

- Para el servidor SQL Express o Microsoft SQL Server, seleccione una de las siguientes opciones:

  - **Modo de autenticación de Microsoft Windows**. La verificación de permisos usa la cuenta utilizada para el inicio del Servidor de administración.

  - **Modo de autenticación de SQL Server**. Si selecciona esta opción, la cuenta especificada en la ventana se usa para verificar los permisos de acceso. Rellene los campos **Cuenta** y **Contraseña**.

    Para ver la contraseña introducida, haga clic y mantenga presionado el botón **Mostrar**.

  Para ambos modos de autenticación, la aplicación comprueba si la base de datos está disponible. Si la base de datos no está disponible, se muestra un mensaje de error y debe proporcionar las credenciales correctas.

  Si la base de datos del Servidor de administración se almacena en otro dispositivo y la cuenta del Servidor de administración no tiene el acceso al servidor de la base de datos, debe usar el modo de autenticación de SQL Server al instalar o actualizar el Servidor de administración. Esto puede ocurrir cuando el dispositivo que almacena la base de datos se encuentra fuera del dominio o cuando el Servidor de administración está instalado en la cuenta LocalSystem.

Para MySQL, MariaDB, PostgreSQL o Postgres Pro, especifique la cuenta y la contraseña.

# Paso 13. Seleccionar la cuenta para iniciar el Servidor de administración

Seleccione la cuenta que será usada para iniciar el Servidor de administración como un servicio.

- **Generar automáticamente la cuenta**. La aplicación crea una cuenta llamada KL-AK-* en la que se ejecutará el servicio kladminserver.

  Puede seleccionar esta opción si planea localizar la carpeta compartida y el DBMS en el mismo dispositivo que el Servidor de administración.

- **Seleccione una cuenta**. El servicio del Servidor de administración (kladminserver) se ejecutará en la cuenta que seleccionó.

  Tendrá que seleccionar una cuenta de dominio si, por ejemplo, planea usar como DBMS una instancia de SQL Server de alguna versión, incluido SQL Express, que se encuentra en otro dispositivo o está planeando localizar la carpeta compartida en otro dispositivo.

  Kaspersky Security Center es compatible con cuentas de servicios administrados (MSA) y cuentas de servicios administrados en grupo (gMSA). Si se utilizan estos tipos de cuentas en su dominio, puede seleccionar una de ellas como la cuenta para el servicio del Servidor de administración.

  Antes de especificar las MSA o las gMSA, debe instalar la cuenta en el mismo dispositivo en el que desea instalar el Servidor de administración. Si la cuenta aún no está instalada, cancele la instalación del Servidor de administración, instale la cuenta y, luego, reinicie la instalación del Servidor de administración. Para obtener más información sobre la instalación de cuentas de servicio administradas en un dispositivo local, consulte la documentación oficial de Microsoft.

  *Para especificar las MSA o las gMSA:*

  1. Haga clic en el botón **Examinar**.
  2. En la ventana que se abre, haga clic en el botón **Tipo de objeto**.
  3. Seleccione **Cuenta para servicios** escriba y haga clic en **Aceptar**.
  4. Seleccione la cuenta relevante y haga clic en **Aceptar**.

La cuenta que seleccionó debe tener permisos diferentes, según qué DBMS planea usar.

Por razones de seguridad, no asigne el estado privilegiado a la cuenta en la cual ejecuta el Servidor de administración.

La cuenta del Servidor de administración no se puede cambiar posteriormente. Debe reinstalar el clúster de conmutación por error para utilizar otra cuenta del Servidor de administración.

## Paso 14. Selección de una cuenta para ejecutar los servicios de Kaspersky Security Center

Seleccione la cuenta a través de la cual los servicios de Kaspersky Security Center se ejecutarán en este dispositivo:

- **Generar automáticamente la cuenta**. Kaspersky Security Center crea una cuenta local denominada KlScSvc en este dispositivo en el grupo kladmins. Los servicios de Kaspersky Security Center se ejecutarán con la cuenta que se ha creado.

- **Seleccione una cuenta**. Los servicios de Kaspersky Security Center se ejecutarán en la cuenta que seleccionó.

  Deberá seleccionar una cuenta de dominio si, por ejemplo, tiene la intención de guardar informes a una carpeta ubicada en un dispositivo diferente o si esto es un requisito de la directiva de seguridad de su organización. También es posible que deba seleccionar una cuenta de dominio si instala el Servidor de administración en un clúster de conmutación por error.

Por razones de seguridad, no conceda estado privilegiado a la cuenta en la cual se ejecutan los servicios.

El servicio del proxy de KSN (ksnproxy), el servicio de proxy de activación de Kaspersky (klactprx) y el servicio del portal de autenticación de Kaspersky (klwebsrv) se ejecutarán en la cuenta seleccionada.

## Paso 15. Seleccionar una carpeta compartida

Defina la ubicación y el nombre de la carpeta compartida que se usará para realizar lo siguiente:

- Almacenar los archivos necesarios para la instalación remota de aplicaciones (los archivos se copian al Servidor de administración durante la creación de los paquetes de instalación).

- Almacenar actualizaciones que se han descargado de un origen de actualizaciones al Servidor de administración.

El uso compartido de archivos (solo lectura) estará habilitado para todos los usuarios.

Puede seleccionar cualquiera de las siguientes opciones:

- **Crear una carpeta compartida**. Crear una nueva carpeta. En el cuadro de texto, especifique la ruta a la carpeta.

- **Seleccionar una carpeta compartida existente**. Seleccione una carpeta compartida que ya exista.

La carpeta compartida puede ser una carpeta local en el dispositivo usado para la instalación o un directorio remoto en cualquier dispositivo cliente dentro de la red corporativa. Se puede usar el botón **Examinar** para seleccionar la carpeta compartida o especificarla de forma manual al ingresar la ruta UNC (por ejemplo, \\server\Share) en el campo correspondiente.

De manera predeterminada, el instalador crea una subcarpeta KLSHARE local en la carpeta de la aplicación que contiene los componentes de Kaspersky Security Center.

Puede definir una carpeta compartida posteriormente si es necesario.

# Paso 16. Configurar la conexión al Servidor de administración

Configurar la conexión con el Servidor de administración:

- **Puerto**

  El número de puerto utilizado para conectar con el Servidor de administración.

  El número de puerto predeterminado es 14000.

- **Puerto SSL**

  El número de puerto SSL (Capa de sockets seguros) se usa para conectarse de manera segura al Servidor de administración mediante SSL.

  El número de puerto predeterminado es 13000.

- **Longitud de la clave de cifrado**

  Seleccione la longitud de la clave de cifrado: 1024 bits o 2048 bits.

  Una clave de cifrado de 1024 bits aplica una carga más pequeña en la CPU, pero se considera obsoleta porque no puede proporcionar cifrado confiable debido a sus especificaciones técnicas. Además, el hardware existente probablemente resultará incompatible con certificados de SSL que presentan claves de 1024 bits.

  Una clave de cifrado de 2048 bits cumple todos los estándares del cifrado de última generación. Sin embargo, el uso de una clave de cifrado de 2048 bits puede aumentar la carga en la CPU.

  Por defecto, **2048 bits (mayor seguridad)** está seleccionado.

También puede cambiar los parámetros para conectarse al Servidor de administración más adelante de la siguiente manera:

- Puede cambiar el puerto y los números de puerto SSL en la sección **Puertos de conexión** de las propiedades del Servidor de administración. Para obtener más información sobre los puertos de conexión del Servidor de administración, consulte Puertos utilizados por Kaspersky Security Center.

- Puede cambiar la longitud de la clave de cifrado cuando reemplaza el certificado del Servidor de administración con la utilidad klsetsrvcert mediante el parámetro `-o RsaKeyLen:<longitud de la clave>`.

## Paso 17. Definir la dirección del Servidor de administración

Definir la dirección del Servidor de administración. Puede seleccionar una de las siguientes opciones:

- **Nombre de dominio DNS**. Puede utilizar este método si la red incluye un servidor DNS y los dispositivos cliente pueden utilizarlo para recibir la dirección del Servidor de administración.
- **Nombre NetBIOS**. Puede utilizar este método si los dispositivos cliente reciben la dirección del Servidor de administración mediante el protocolo NetBIOS o si hay un servidor WINS disponible en la red.
- **Dirección IP**. Puede utilizar este método si el Servidor de administración tiene una dirección IP estática que no se modificará posteriormente.

## Paso 18. Dirección del Servidor de administración para la conexión de dispositivos móviles

Este paso del asistente de instalación se encuentra disponible si ha seleccionado la Administración de dispositivos móviles para la instalación.

En la ventana **Dirección para la conexión de dispositivos móviles**, especifique la dirección externa del Servidor de administración para la conexión de los dispositivos móviles que están fuera de la red local. Puede especificar la dirección IP o el Sistema de nombres de dominio (DNS) del Servidor de administración.

## Paso 19. Desempaquetar e instalar archivos en el disco duro

Después de configurar la instalación de los componentes de Kaspersky Security Center, puede comenzar con la instalación de archivos en el disco duro.

Si la instalación requiere programas adicionales, el asistente de instalación se lo notificará en la página **Instalando requisitos previos** antes de instalar Kaspersky Security Center. Los programas requeridos se instalarán automáticamente después de hacer clic en el botón **Siguiente**.

En la última página, puede seleccionar qué consola desea iniciar para trabajar con Kaspersky Security Center:

- **Iniciar Consola de administración basada en MMC**
- **Iniciar Kaspersky Security Center Web Console**

  Esta opción solo está disponible si ha optado por instalar Kaspersky Security Center Web Console en uno de los pasos anteriores.

También puede hacer clic en **Finalizar** para cerrar el asistente sin comenzar a trabajar con Kaspersky Security Center. Puede iniciar el trabajo más tarde en cualquier momento.

Al iniciar por primera vez la Consola de administración o Kaspersky Security Center Web Console, puede realizar la configuración inicial de la aplicación.

# Instalación del Servidor de administración en modo no interactivo

El Servidor de administración puede instalarse en modo no interactivo; es decir, sin entrada interactiva de la configuración de instalación.

*Para instalar el Servidor de administración en un dispositivo local en modo no interactivo:*

1. Lea el Contrato de licencia de usuario final. Use el comando a continuación únicamente si comprende y acepta los términos del Contrato de licencia de usuario final.

2. Leer la Política de privacidad. Este parámetro confirma que es consciente y está de acuerdo con que sus mis datos serán manejados y transmitidos (incluso a terceros países) como se describe en la Política de privacidad.

3. Ejecute el comando
   `setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVACYPOLICY=1 <setup_parameters>"`

donde `parámetros_de_instalación` es una lista de parámetros y sus valores correspondientes separados por espacios (`PARAM1=PARAM1VAL PARAM2=PARAM2VAL`). El archivo setup.exe se ubica en la carpeta Servidor, que es parte del kit de distribución de Kaspersky Security Center.

Los nombres y posibles valores de los parámetros que pueden usarse al instalar el Servidor de administración en modo no interactivo se mencionan en la tabla a continuación.

Parámetros de instalación del Servidor de administración en modo no interactivo

| Nombre del parámetro | Descripción del parámetro | Valores disponibles |
|---|---|---|
| EULA | Aceptación de los términos del Contrato de licencia. | • 1: he leído, comprendo y acepto en su totalidad los términos del Contrato de licencia de usuario final.<br>• Otro valor o ningún valor: no acepto los términos del Contrato de licencia (no se realizará la instalación). |
| PRIVACYPOLICY | Aceptación de los términos de la Política de privacidad. | • 1: entiendo y acepto que mis datos serán tratados y transmitidos (incluso a otros países) según lo descrito en la Política de privacidad. Confirmo que he leído y que comprendo en su totalidad la Política de privacidad.<br>• Otro valor o ningún valor: no acepto los términos de la Política de privacidad (no se realizará la instalación). |
| INSTALLATIONMODETYPE | Tipo de instalación del Servidor de administración. | • Standard: instalación estándar.<br>• Custom: instalación personalizada. |
| INSTALLDIR | Ruta a la carpeta de instalación del Servidor de administración. | Valor de cadena. |
| ADDLOCAL | Lista de los componentes del Servidor de administración (separados por comas) que se deben instalar. | CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86.<br>Lista mínima de componentes que se requieren para instalar el Servidor de administración:<br>`ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`. |

| Nombre del parámetro | Descripción del parámetro | Valores disponibles |
|---|---|---|
| NETRANGETYPE | Tamaño de la red (número de dispositivos en la red). | • NRT_1_100: de 1 a 100 dispositivos.<br>• NRT_100_1000: de 101 a 1000 dispositivos.<br>• NRT_GREATER_1000: más de 1 000 dispositivos. |
| SRV_ACCOUNT_TYPE | Modo de especificación de una cuenta bajo la que el Servidor de administración se ejecutará como un servicio. | • SrvAccountDefault: la cuenta se crea automáticamente.<br>• SrvAccountUser: la cuenta se define manualmente. En este caso, debe especificar valores para los parámetros `SERVERACCOUNTNAME` y `SERVERACCOUNTPWD`. |
| SERVERACCOUNTNAME | Nombre de la cuenta mediante la que se ejecutará el Servidor de administración como servicio. Debe especificar un valor para el parámetro si SRV_ACCOUNT_TYPE=SrvAccountUser. | Valor de cadena. |
| SERVERACCOUNTPWD | Contraseña de la cuenta que será usada para iniciar el Servidor de administración como un servicio. Debe especificar un valor para el parámetro si SRV_ACCOUNT_TYPE=SrvAccountUser. | Valor de cadena. |
| SERVERCER | Tamaño de la clave del certificado del Servidor de administración (bits). | • 1: El tamaño de la clave para el certificado del Servidor de administración es de 2048 bits.<br>• Sin valor: El tamaño de la clave para el certificado del Servidor de administración es de 1024 bits. |
| DBTYPE | Tipo de base de datos que se utilizará para almacenar la base de datos del Servidor de administración.<br>Este parámetro es obligatorio. | • MySQL: se utilizará una base de datos MySQL o MariaDB. En este caso, debe especificar valores para los parámetros `MYSQLSERVERNAME`, `MYSQLSERVERPORT`, `MYSQLDBNAME`, `MYSQLACCOUNTNAME` y `MYSQLACCOUNTPWD`.<br>• MSSQL: se usará la base de datos de Microsoft SQL Server (SQL Express). En este caso, debe especificar valores para los parámetros `MSSQLSERVERNAME`, `MSSQLDBNAME` y `MSSQLAUTHTYPE`.<br>• POSTGRES: se utilizará una base de datos PostgreSQL o Postgres Pro. En este caso, debe especificar valores para los parámetros `POSTGRESSERVERNAME`, `POSTGRESSERVERPORT`, `POSTGRESDBNAME`, `POSTGRESACCOUNTNAME` y `POSTGRESACCOUNTPWD`. |
| MYSQLSERVERNAME | Nombre completo de SQL Server. Debe especificar un valor para el parámetro si DBTYPE=MySQL. | Valor de cadena. |
| MYSQLSERVERPORT | Número del puerto para conectar al SQL Server. Debe especificar un valor para el parámetro si DBTYPE=MySQL. | Valor numérico. |
| MYSQLDBNAME | Nombre de la base de datos que se creará para almacenar los datos del Servidor de administración. Debe especificar un valor para el parámetro si DBTYPE=MySQL. | Valor de cadena. |
| MYSQLACCOUNTNAME | Nombre de la cuenta para conectarse a la base de datos. Debe especificar un valor para el parámetro si DBTYPE=MySQL. | Valor de cadena. |
| MYSQLACCOUNTPWD | Contraseña de la cuenta para conectarse a la base de datos. Debe especificar un valor para el parámetro si DBTYPE=MySQL. | Valor de cadena. |
| MSSQLSERVERNAME | Nombre completo de SQL Server. Debe especificar un valor para el parámetro si DBTYPE=MSSQL. | Valor de cadena. |
| MSSQLDBNAME | Nombre de la base de datos. Debe especificar un valor para el parámetro si DBTYPE=MSSQL. | Valor de cadena. |

| Nombre del parámetro | Descripción del parámetro | Valores disponibles |
|---|---|---|
| MSSQLAUTHTYPE | Tipo de autorización para conectar al SQL Server. Debe especificar un valor para el parámetro si DBTYPE=MSSQL. | • Windows: modo de autenticación de Microsoft Windows.<br>• SQLServer: modo de autenticación de SQL Server. En este caso, debe especificar valores para los parámetros `MSSQLACCOUNTNAME` y `MSSQLACCOUNTPWD`. |
| MSSQLACCOUNTNAME | Nombre de la cuenta para conectar al SQL Server. Debe especificar un valor para el parámetro si MSSQLAUTHTYPE=SQLServer. | Valor de cadena. |
| MSSQLACCOUNTPWD | Contraseña de la cuenta para conectar al SQL Server. Debe especificar un valor para el parámetro si MSSQLAUTHTYPE=SQLServer. | Valor de cadena. |
| CREATE_SHARE_TYPE | Método de especificación de la carpeta compartida. | • Create: Crear una carpeta compartida nueva. En este caso, debe especificar valores para los parámetros `SHARELOCALPATH` y `SHAREFOLDERNAME`.<br>• ChooseExisting: seleccione una carpeta existente. En este caso, debe especificar un valor para el parámetro `EXISTSHAREFOLDERNAME`. |
| SHARELOCALPATH | Ruta de acceso completa de la carpeta local. Debe especificar un valor para el parámetro si CREATE_SHARE_TYPE=Create. | Valor de cadena. |
| SHAREFOLDERNAME | Nombre de la red de una carpeta compartida. Debe especificar un valor para el parámetro si CREATE_SHARE_TYPE=Create. | Valor de cadena. |
| EXISTSHAREFOLDERNAME | Ruta completa a una carpeta compartida existente.<br>Debe especificar un valor para el parámetro si CREATE_SHARE_TYPE=ChooseExisting. | Valor de cadena. |
| SERVERPORT | Número de puerto utilizado para conectarse al Servidor de administración. | Valor numérico. |
| SERVERSSLPORT | Número del puerto para conexión cifrada al Servidor de administración usando el protocolo SSL. | Valor numérico. |
| SERVERADDRESS | Dirección de Servidor de administración. | Valor de cadena. |
| MOBILESERVERADDRESS | Dirección externa del Servidor de administración para la conexión de dispositivos móviles. | Valor de cadena. |

Para obtener una descripción detallada de los parámetros de instalación del Servidor de administración, consulte la sección Instalación personalizada.

# Instalación de la Consola de administración en la estación de trabajo del administrador

La Consola de administración se puede instalar por separado en la estación de trabajo del administrador y el Servidor de administración se puede administrar por la red usando esa consola.

*Para instalar la Consola de administración en la estación de trabajo del administrador:*

1. Ejecute el archivo ejecutable setup.exe.

   Se abre una ventana y se le solicita que seleccione las aplicaciones de Kaspersky que desea instalar.

2. En la ventana de selección de aplicaciones, haga clic en el vínculo **Instalar solo la Consola de administración de Kaspersky Security Center** para ejecutar el Asistente de instalación de la Consola de administración. Siga las instrucciones del asistente.

3. Seleccione una carpeta de destino. De manera predeterminada, la carpeta es <Unidad>:\Archivos de programa\Kaspersky Lab\Kaspersky Security Center Console. Si la carpeta no existe, se crea automáticamente durante la instalación. Es posible cambiar la carpeta de destino usando el botón **Examinar**.

4. En la última página del Asistente de instalación, haga clic en el botón **Iniciar** para iniciar la instalación de la Consola de administración.

Cuando finalice el Asistente, la Consola de administración estará instalada en la estación de trabajo del administrador.

*Para instalar la Consola de administración en la estación de trabajo del administrador en modo no interactivo:*

1. Lea el Contrato de licencia de usuario final. Use el comando a continuación únicamente si comprende y acepta los términos del Contrato de licencia de usuario final.

2. En la carpeta `Distrib\Console` del kit de distribución de Kaspersky Security Center, ejecute el archivo setup.exe con el siguiente comando:

   ```
   setup.exe /s /v"EULA=1"
   ```

   Si desea instalar todos los complementos de administración de la carpeta `Distrib\Console\Plugins` junto con la Consola de administración, ejecute el siguiente comando:

   ```
   setup.exe /s /v"EULA=1" /pALL
   ```

   Si desea especificar qué complementos de administración instalar desde la carpeta `Distrib\Console\Plugins` junto con la Consola de administración, especifique los complementos después de la clave "/p" y sepárelos con un punto y coma:

   ```
   setup.exe /s /v"EULA=1" /pP1;P2;P3
   ```

   donde `P1`, `P2` y `P3` son nombres de complementos que corresponden a los nombres de las carpetas de complementos en la carpeta `Distrib\Console\Plugins`. Por ejemplo:

   ```
   setup.exe /s /v"EULA=1" /pKES4Mac;KESS;MDM4IOS
   ```

La Consola de administración y los complementos de administración (si los hubiera) se instalarán en la estación de trabajo del administrador.

Después de instalar la Consola de administración, debe conectarse al Servidor de administración. Para hacerlo, ejecute la Consola de administración y, en la ventana que se abrirá, especifique el nombre o la dirección IP del dispositivo en el que el Servidor de administración está instalado y la configuración de la cuenta usada para conectarse a él. Después de establecer la conexión con el Servidor de administración, puede administrar el sistema de protección antivirus usando esta Consola de administración.

La Consola de administración se puede eliminar con las herramientas de adición y eliminación estándares de Microsoft Windows.

# Cambios en el sistema después de la instalación de Kaspersky Security Center

## Icono de la Consola de administración

Después de haber instalado la Consola de administración en su dispositivo, aparecerá el icono que se usa para iniciar la Consola. Puede acceder a la Consola de administración desde **Inicio** → **Programas** → menú **Kaspersky Security Center**.

## Servicios del Servidor de administración y el Agente de red

El Servidor de administración y el Agente de red se instalarán en el dispositivo como servicios con las propiedades que se detallan a continuación. La tabla también contiene los atributos de otros servicios que se implementan en el dispositivo después de instalar el Servidor de administración.

Propiedades de los servicios de Kaspersky Security Center

| Componente | Nombre del servicio | Nombre del servicio que se muestra | Cuenta |
|---|---|---|---|
| Servidor de administración | kladminserver | Servidor de administración de Kaspersky Security Center | Cuenta sin privilegios dedicada o definida por el usuario con formato KL-AK-* creada durante la instalación |
| Agente de red | klnagent | Agente de red de Kaspersky Security Center | Sistema local |
| Servidor web para acceder a Kaspersky Security Center Web Console y administrar la intranet de la organización | klwebsrv | Servidor web de Kaspersky | Cuenta dedicada KlScSvc sin privilegios |
| Servidor proxy de activación | klactprx | Servidor proxy de activación de Kaspersky | Cuenta dedicada KlScSvc sin privilegios |
| Servidor proxy de KSN | ksnproxy | Servidor proxy de Kaspersky Security Network | Cuenta dedicada KlScSvc sin privilegios |

Si instala Kaspersky Security Center en los nodos del clúster de conmutación por error de Kaspersky Security Center, el servicio klfocsvc_klfoc estará disponible. Los servicios klnagent_klfoc y klfocsvc_klfoc se ejecutan en la cuenta del sistema local. El servicio kladminserver_klfoc debe ejecutarse con la cuenta "ksc" y los demás servicios se deben ejecutar con la cuenta "sin derechos". Las cuentas "ksc" y "sin derechos" deben agregarse al grupo KLAdmins con los permisos del administrador local. Para que Kaspersky Security Center funcione de forma correcta, solo debe usar las cuentas "ksc" y "sin derechos" para ejecutar los servicios. No recomendamos usar otras cuentas con los mismos derechos. La siguiente tabla contiene las propiedades de los servicios que se aplican al dispositivo después de instalar el Servidor de administración en el clúster de conmutación por error de Kaspersky Security Center.

Propiedades de los servicios de Kaspersky Security Center instalados en el clúster de conmutación por error de Kaspersky Security Center

| Componente | Nombre del servicio | Nombre del servicio que se muestra | Cuenta |
|---|---|---|---|
| Servidor de administración | kladminserver_klfoc | Servidor de administración de Kaspersky Security Center | ksc |
| Agente de red | klnagent_klfoc | Agente de red de Kaspersky Security Center | Sistema local |

| | | | |
|---|---|---|---|
| Servidor web para acceder a Kaspersky Security Center Web Console y administrar la intranet de la organización | klwebsrv_klfoc | Servidor web de Kaspersky | sin derechos |
| Servidor proxy de activación | klactprx_klfoc | Servidor proxy de activación de Kaspersky | sin derechos |
| Servidor proxy de KSN | ksnproxy_klfoc | Servidor proxy de Kaspersky Security Network | sin derechos |
| Clúster de conmutación por error de Kaspersky Security Center | klfocsvc_klfoc | Clúster de conmutación por error de Kaspersky Security Center | Sistema local |

## Servicios de Kaspersky Security Center Web Console

Si instala Kaspersky Security Center Web Console en el dispositivo, se implementarán los siguientes servicios (consulte la tabla a continuación):

Servicios de Kaspersky Security Center Web Console

| Nombre del servicio que se muestra | Cuenta |
|---|---|
| Servicio Kaspersky Security Center Web Console | Servicio NT/KSCSvcWebConsole |
| Kaspersky Security Center Web Console | Servicio de red |
| Kaspersky Security Center Product Plugins Server | Servicio NT/KSCWebConsolePlugin |
| Servicio de administración de Kaspersky Security Center Web Console | Sistema local |
| Cola de mensajes de Kaspersky Security Center Web Console | Servicio NT/KSCWebConsoleMessageQueue |

## Versión del servidor del Agente de red

La versión de servidor del Agente de red se instalará en el dispositivo junto con el Servidor de administración. La versión de servidor del Agente de red es parte del Servidor de administración, se instala y se elimina junto con el Servidor de administración y solo puede interactuar con un Servidor de administración instalado de forma local. No es necesario configurar la conexión del Agente de red al Servidor de administración: la configuración se implementa programáticamente porque los componentes están instalados en el mismo dispositivo. La versión del servidor del Agente de red se instala con las mismas propiedades que el Agente de red estándar y ejecuta las mismas funciones de administración de aplicaciones. Esta versión será administrada por la directiva del grupo de administración al que pertenece el dispositivo cliente del Servidor de administración. Para la versión de servidor del Agente de red, todas las tareas se crean a partir del alcance de las tareas proporcionadas para el Servidor de administración, excepto la tarea de modificación del servidor.

El Agente de red no se puede instalar por separado en un dispositivo que ya tiene el Servidor de administración instalado.

Usted puede ver las propiedades de cada servicio del Servidor de administración y del Agente de red, además de supervisar su funcionamiento mediante las herramientas estándar de administración de Microsoft Windows: Administración de equipos\Servicios. La información sobre la actividad del servicio del Servidor de administración de Kaspersky se almacena en el registro del sistema de Microsoft Windows, en una rama separada del Registro de eventos de Kaspersky en el dispositivo donde está instalado el Servidor de administración.

Recomendamos que evite iniciar y detener servicios manualmente y que deje las cuentas de servicio en la configuración del servicio sin alterar. Si es necesario, puede modificar la cuenta de servicio del Servidor de administración con la utilidad klsrvswch. Tenga en cuenta que debe iniciar la utilidad klsrvswch en el dispositivo del Servidor de administración de la cuenta con derechos de administrador que se utilizó para instalar el Servidor de administración.

### Cuentas de usuario y grupos de seguridad

El instalador del Servidor de administración creó las siguientes cuentas de forma predeterminada:

- KL-AK-*: Cuenta de servicio del Servidor de administración
- KlScSvc: Cuenta para otros servicios del grupo del Servidor de administración
- KlPxeUser: Cuenta para el despliegue de sistemas operativos

Si seleccionó otras cuentas para el servicio del Servidor de administración y otros servicios al ejecutar el Instalador, se utilizan las cuentas especificadas.

Los grupos de seguridad locales denominados KLAdmins y KLOperators con sus correspondientes conjuntos de derechos también se crean automáticamente en el dispositivo que tiene instalado el Servidor de administración.

No se recomienda instalar el Servidor de administración en un controlador de dominio. Sin embargo, si instala el Servidor de administración en el controlador de dominio, deberá iniciar el instalador con los derechos de administrador de dominio. En este caso, el instalador crea automáticamente grupos de seguridad de dominio denominados KLAdmins y KLOperators. Si instala el Servidor de administración en un dispositivo que no es el controlador de dominio, debe iniciar el instalador con los derechos de administrador local. En este caso, el instalador crea automáticamente grupos de seguridad locales denominados KLAdmins y KLOperators.

Al configurar las notificaciones por correo electrónico, es posible que deba crear una cuenta en el servidor de correo para la autenticación ESMTP.

## Eliminando la aplicación

Puede eliminar Kaspersky Security Center con herramientas estándar para agregar y quitar aplicaciones de Microsoft Windows. Eliminar la aplicación requiere iniciar un Asistente que elimina todos los componentes de la aplicación desde el dispositivo (incluidos los complementos). El Asistente hace que su navegador predeterminado abra una página web con una encuesta en la que puede decirnos por qué decidió dejar de usar Kaspersky Security Center. Si no seleccionó la eliminación de la carpeta compartida (KLSHARE) durante el funcionamiento del Asistente, puede eliminarla manualmente después de completar todas las tareas relacionadas.

Después de que la aplicación se elimina, algunos de sus archivos pueden permanecer en la carpeta temporal del sistema.

El Asistente para la creación de tareas de eliminación de aplicaciones le sugerirá que almacene una copia de seguridad del Servidor de administración.

Al eliminar la aplicación de Microsoft Windows 7 y Microsoft Windows 2008, es posible que el Asistente para la creación de tareas de eliminación de aplicaciones finalice prematuramente. Esto se puede evitar al deshabilitar el Control de Cuenta de Usuario (UAC) en el sistema operativo y reiniciar la desinstalación de la aplicación.

# Acerca de las actualizaciones de versión en Kaspersky Security Center

En esta sección, encontrará información para actualizar la versión de Kaspersky Security Center. Puede actualizar Kaspersky Security Center de diferentes maneras, según si Kaspersky Security Center se instaló de forma local o en los nodos del clúster de conmutación por error de Kaspersky Security Center.

Durante la actualización, es fundamental que el DBMS no sea utilizado simultáneamente por el Servidor de administración y por otras aplicaciones.

Tenga en cuenta que si actualiza el Servidor de administración a la versión 15.1, no podrá crear nuevos paquetes de instalación del Agente de red versión 15 ni versiones anteriores. Sin embargo, los paquetes de instalación creados anteriormente estarán disponibles.

Cuando se instala una versión actualizada de Kaspersky Security Center, se conservan los complementos instalados para las aplicaciones de Kaspersky compatibles. El complemento del Servidor de administración y el complemento del Agente de red se actualizan automáticamente (tanto para la Consola de administración como para Kaspersky Security Center 14 Web Console).

# Actualización de Kaspersky Security Center desde una versión anterior

El siguiente tema describe los pasos de preparación recomendados para la actualización: Actualización de Kaspersky Security Center y aplicaciones de seguridad administradas.

Puede instalar la versión 15.1 del Servidor de administración en un dispositivo que tenga una versión anterior del Servidor de administración instalada (a partir de la versión 11 [11.0.0.1131b]). Al actualizar a la versión 15.1, se conservan todos los datos y configuraciones de la versión anterior del Servidor de administración.

Si ocurre un problema durante la instalación del Servidor de administración, se puede restaurar la versión anterior del Servidor de administración mediante la copia de seguridad de los datos del Servidor de administración creada antes de la actualización.

Si se instaló al menos un Servidor de administración de la nueva versión en la red, puede actualizar otros Servidores de administración en la red mediante la tarea de instalación remota que utiliza el paquete de instalación del Servidor de administración.

Si implementó el clúster de conmutación por error de Kaspersky Security Center, también puede actualizar Kaspersky Security Center en los nodos que lo conforman.

*Para actualizar una versión anterior del Servidor de administración a la versión 15.1, realice lo siguiente:*

1. Ejecute el archivo de instalación ksc_<número de versión>_<número de compilación>_full_<idioma>.exe de la versión 14 (puede descargarlo del sitio web de Kaspersky).

2. En la ventana que se abre, haga clic en el vínculo **Instalar Kaspersky Security Center** para iniciar el Asistente de instalación del Servidor de administración. Siga las instrucciones del asistente.

3. Lea el Contrato de licencia y la Política de privacidad. Si está de acuerdo con todos los términos del Contrato de licencia y la Política de privacidad, seleccione las casillas siguientes en la sección **Confirmo que he leído y comprendido la totalidad del texto, y que acepto lo siguiente**:

   - **Los términos y las condiciones de este EULA**
   - **la Política de privacidad que describe el manejo de los datos**

   La instalación de la aplicación en su dispositivo continuará después de que seleccione ambas casillas. El Asistente de instalación le ofrecerá crear una copia de seguridad con los datos de la versión anterior del Servidor de administración.

   Kaspersky Security Center puede recuperar los datos de una copia de seguridad creada con una versión más antigua del Servidor de administración.

4. Si desea crear una copia de seguridad de los datos del Servidor de administración, indíquelo en la ventana que se abre, **Copia de seguridad de los datos del Servidor de administración**.

   Las copias de seguridad se crean con la utilidad klbackup. Esta utilidad está incluida en el kit de distribución; la encontrará en la raíz de la carpeta de instalación de Kaspersky Security Center.

5. Siga las instrucciones del Asistente de instalación para instalar la versión 15.1 del Servidor de administración.

   Si se le indica que el servicio de Kaspersky Security Center 14 Web Console está ocupado, haga clic en el botón **Ignorar** de la ventana del asistente.

   Le recomendamos que evite finalizar el Asistente de instalación. Si cancela la actualización mientras el Servidor de administración se está instalando, la versión actualizada de Kaspersky Security Center podría no funcionar correctamente.

6. Para dispositivos que tienen instalada una versión anterior del Agente de red, cree y ejecute la tarea de instalación remota para la nueva versión del Agente de red.

   Le recomendamos que actualice el Agente de red para Linux a la misma versión que Kaspersky Security Center.

   La versión actualizada del Agente de red se instalará una vez que se complete la tarea de instalación remota.

   Ejecute los siguientes comandos en activos basados en Linux para eliminar las dependencias que ya no son necesarias:

   - Para activos basados en Debian, ejecute cualquiera de los siguientes comandos:
     - `apt-get -y autoremove`
     - `apt -y autoremove`
   - Para activos basados en RPM, ejecute cualquiera de los siguientes comandos:
     - `dnf autoremove`
     - `yum autoremove`

# Actualización de Kaspersky Security Center en los nodos del clúster de conmutación por error de Kaspersky Security Center

Puede instalar la versión 15.1 del Servidor de administración en cada nodo del clúster de conmutación por error de Kaspersky Security Center que tenga instalada una versión más antigua del Servidor de administración (excepto versiones anteriores a la 13.2). Al actualizar a la versión 15.1, se conservan todos los datos y configuraciones de la versión anterior del Servidor de administración.

Si tiene dispositivos en los que ha instalado Kaspersky Security Center de manera local, también puede actualizar en ellos la versión de Kaspersky Security Center.

*Para actualizar Kaspersky Security Center en los nodos del clúster de conmutación por error de Kaspersky Security Center, siga estos pasos:*

1. Realice las siguientes acciones en el nodo activo del clúster:

   a. Ejecute el archivo ejecutable ksc_15.1_ <número de compilación> _full_ <idioma> .exe.

   Se abre una ventana en la que debe elegir las aplicaciones de Kaspersky que desea actualizar. Haga clic en el vínculo **Instalar el Servidor de administración de Kaspersky Security Center** para iniciar el asistente de instalación del Servidor de administración. Siga las instrucciones del asistente.

   b. Lea el Contrato de licencia y la Política de privacidad. Si está de acuerdo con todos los términos del Contrato de licencia y la Política de privacidad, seleccione las casillas siguientes en la sección **Confirmo que he leído y comprendido la totalidad del texto, y que acepto lo siguiente**:

   - **Los términos y las condiciones de este EULA**
   - **la Política de privacidad que describe el manejo de los datos**

   Marque ambas casillas para continuar con la instalación.

   Si no está de acuerdo con el Contrato de licencia o con la Política de privacidad, haga clic en el botón **Cancelar** para cancelar la actualización.

2. Realice las mismas acciones en el nodo pasivo del clúster de conmutación por error de Kaspersky Security Center que en el nodo activo.

3. Inicie el clúster.

Como resultado, instaló la versión más reciente del Servidor de administración en los nodos del clúster de conmutación por error de Kaspersky Security Center.

# Actualizar Kaspersky Security Center en los nodos de un clúster de conmutación por error de Microsoft

Puede actualizar la versión 15.1 del Servidor de administración en cada nodo de un clúster de conmutación por error de Microsoft que cuente con una versión más antigua del Servidor de administración (excepto versiones anteriores a la 13.2). Al actualizar a la versión 15.1, se conservan todos los datos y configuraciones de la versión anterior del Servidor de administración.

*Para actualizar Kaspersky Security Center en los nodos del clúster de conmutación por error de Microsoft, realice las siguientes acciones en cualquier nodo del clúster:*

1. Ejecute el archivo ejecutable ksc_15.1_ <número de compilación> _full_ <idioma> .exe.

   Se abre una ventana en la que debe elegir las aplicaciones de Kaspersky que desea actualizar. Haga clic en el vínculo **Instalar el Servidor de administración de Kaspersky Security Center** para iniciar el asistente de instalación del Servidor de administración. Siga las instrucciones del asistente.

2. Lea el Contrato de licencia y la Política de privacidad. Si está de acuerdo con todos los términos del Contrato de licencia y la Política de privacidad, seleccione las casillas siguientes en la sección **Confirmo que he leído y comprendido la totalidad del texto, y que acepto lo siguiente**:

   - **Los términos y las condiciones de este EULA**
   - **la Política de privacidad que describe el manejo de los datos**

   Marque ambas casillas para continuar con la instalación.

   Si no está de acuerdo con el Contrato de licencia o con la Política de privacidad, haga clic en el botón **Cancelar** para cancelar la actualización.

3. En la ventana **Tipo de instalación en clúster**, seleccione **Clúster (instalar en todos los nodos del clúster)**.

   A continuación, el instalador configura y finaliza la actualización del Servidor de administración en todos los nodos del clúster. Durante la actualización, la configuración del Servidor de administración no se puede cambiar.

Al concluir este procedimiento, los nodos del clúster de conmutación por error de Microsoft contarán con la versión más reciente del Servidor de administración.

# Configuración inicial de Kaspersky Security Center

Esta sección describe los pasos que debe seguir después de la instalación de Kaspersky Security Center para realizar su configuración inicial.

## Guía para reforzar la seguridad

La Guía para reforzar la seguridad está dirigida a los profesionales que instalan y administran Kaspersky Security Center, así como para los que proporcionan soporte técnico a las organizaciones que utilizan Kaspersky Security Center.

La Guía para reforzar la seguridad describe recomendaciones y funciones para configurar Kaspersky Security Center y sus componentes, con el objetivo de reducir los riesgos de compromiso.

Antes de la configuración, cree una copia de seguridad del Servidor de administración de Kaspersky Security Center con la tarea Copia de seguridad de los datos del Servidor de administración o la utilidad klbackup y guárdela en un lugar seguro.

La Guía para reforzar la seguridad incluye la siguiente información:

- Selección de la arquitectura del Servidor de administración
- Configuración de una conexión segura al Servidor de administración

- Configuración de las cuentas para acceder al Servidor de administración
- Administración de la protección del Servidor de administración y los dispositivos cliente
- Configurar la protección para aplicaciones administradas
- Mantenimiento del Servidor de administración
- Transferencia de información a aplicaciones de terceros

Antes de comenzar a trabajar con el Servidor de administración, Kaspersky Security Center le pide que lea la versión breve de la Guía para reforzar la seguridad.

Tenga en cuenta que no puede usar el Servidor de administración hasta que confirme que ha leído la Guía para reforzar la seguridad.

*Para leer la Guía para reforzar la seguridad:*

1. Abra la Consola de administración o Kaspersky Security Center Web Console e inicie sesión en la consola. La consola verifica si confirmó haber leído la versión actual de la Guía para reforzar la seguridad.

   Si aún no ha leído la Guía para reforzar la seguridad, se abre una ventana y aparece una versión breve de la misma.

2. Realice una de las siguientes acciones:

   - Si desea ver la versión breve de la Guía para reforzar la seguridad como documento de texto, haga clic en el vínculo **Abrir en una ventana nueva**.
   - Si desea ver la versión completa de la Guía para reforzar la seguridad, haga clic en el vínculo **Abrir la guía para reforzar la seguridad en la Ayuda en línea**.

3. Tras leer la Guía para reforzar la seguridad, seleccione la casilla **Confirmo que he leído y que comprendo en su totalidad la guía para reforzar la seguridad** y, a continuación, haga clic en el botón **Aceptar**.

Ahora puede trabajar con el Servidor de administración.

Cuando aparece una nueva versión de la Guía para reforzar la seguridad, Kaspersky Security Center le solicita que la lea.

# Asistente de inicio rápido del Servidor de administración

Esta sección proporciona información acerca del Asistente de inicio rápido del Servidor de administración.

## Acerca del asistente de inicio rápido

Esta sección proporciona información acerca del Asistente de inicio rápido del Servidor de administración.

Asistente de inicio rápido del Servidor de administración le permite crear un mínimo de tareas y directivas necesarias, ajustar un mínimo de configuraciones, descargar e instalar complementos para aplicaciones administradas de Kaspersky y crear paquetes de instalación de aplicaciones administradas de Kaspersky. Cuando el asistente se está ejecutando, le permite hacer los siguientes cambios en la aplicación:

- Descargue e instale complementos para aplicaciones administradas. Una vez que el Asistente de inicio rápido ha finalizado, la lista de complementos de administración instalados se muestra en la sección **Avanzado** → **Detalles de los complementos de administración de aplicaciones instalados** de la ventana de propiedades del Servidor de administración.

- Crear paquetes de instalación para las aplicaciones de Kaspersky administradas. Una vez finalizado el Asistente de inicio rápido, los paquetes de instalación del Agente de red para Windows y de las aplicaciones de Kaspersky administradas se muestran en la lista **Servidor de administración** → **Avanzado** → **Instalación remota** → **Paquetes de instalación**.

- Agregar archivos de clave o introducir códigos de activación que puedan distribuirse automáticamente a los dispositivos de los grupos de administración. Una vez finalizado el Asistente de inicio rápido, se muestra información sobre las claves de licencia en la lista **Servidor de administración** → **Licencias de Kaspersky** y en la sección **Claves de licencia** de la ventana de propiedades del Servidor de administración.

- Configurar la interacción con Kaspersky Security Network (KSN).

- Configura la entrega mediante correo electrónico de notificaciones de eventos que ocurren durante la operación del Servidor de administración y las aplicaciones administradas (para garantizar la entrega de una notificación exitosa, el servicio de Messenger debe ejecutarse en el Servidor de administración y en todos los dispositivos de destino). Una vez que el Asistente de inicio rápido ha finalizado, la configuración de notificaciones por correo electrónico se muestra en la sección **Notificación** de la ventana de propiedades del Servidor de administración.

- Ajustar los parámetros de actualización y de reparación de vulnerabilidades para las aplicaciones instaladas en los dispositivos.

- Crear una directiva de protección para estaciones de trabajo y servidores, además de tareas de análisis antimalware, tareas de descarga de actualizaciones y tareas de copia de seguridad de datos, para el nivel superior de la jerarquía de dispositivos administrados. Una vez finalizado el Asistente de inicio rápido, las tareas creadas se muestran en la lista **Servidor de administración** → **Tareas**, las directivas correspondientes a los complementos para aplicaciones administradas se muestran en la lista **Servidor de administración** → **Directivas**.

El Asistente de inicio rápido crea directivas para las aplicaciones administradas, como Kaspersky Endpoint Security para Windows, a menos que dichas directivas ya se creen para el grupo de **dispositivos administrados**. El Asistente de inicio rápido crea tareas si no existen tareas con los mismos nombres para el grupo **Dispositivos administrados**.

En la Consola de administración, Kaspersky Security Center le solicita automáticamente que ejecute el Asistente de inicio rápido después de haberlo iniciado por primera vez. El asistente de inicio rápido también se puede ejecutar manualmente en cualquier momento.

## Iniciar el Asistente de inicio rápido del Servidor de administración

La aplicación le preguntará si desea abrir el asistente de inicio rápido cuando termine con la instalación del Servidor de administración y se conecte a este por primera vez. El asistente de inicio rápido también se puede ejecutar manualmente en cualquier momento.

*Para iniciar el asistente de inicio rápido manualmente:*

1. En el árbol de consola, haga clic el nodo del **Servidor de administración**.
2. En el menú contextual del nodo, seleccione **Todas las tareas → Asistente de inicio rápido del Servidor de administración**.

   El asistente le ofrecerá realizar la configuración inicial del Servidor de administración. Siga las instrucciones del asistente.

Si inicia de nuevo el Asistente de inicio rápido, las tareas y directivas creadas en la ejecución anterior del Asistente no podrán volver a crearse.

## Paso 1. Configuración de un servidor proxy

Especifique la configuración de acceso a Internet para el Servidor de administración. Debe configurar el acceso a Internet para usar Kaspersky Security Network y descargar actualizaciones y bases de datos antivirus para Kaspersky Security Center y las aplicaciones de Kaspersky administradas.

Seleccione la opción **Usar servidor proxy** si desea usar un servidor proxy al conectarse a Internet. Si se selecciona esta opción, los campos estarán disponibles para escribir la configuración. Deberá introducir los siguientes valores de conexión del servidor proxy:

- **Dirección**

  Dirección del servidor proxy usado para conectar Kaspersky Security Center con Internet.

- **Número de puerto**

  Número del puerto a través del cual se establecerá la conexión proxy de Kaspersky Security Center.

- **No usar el servidor proxy para direcciones locales**

  Ningún servidor proxy se usará para conectarse a los dispositivos en la red local.

- **Autenticación del servidor proxy**

  Si se selecciona esta casilla, en los campos de entrada se podrán especificar las credenciales para la autenticación del servidor proxy.

  Este campo de entrada está disponible cuando la casilla **Usar servidor proxy** está desmarcada.

- **Nombre de usuario**

  Cuenta de usuario con la que se establece la conexión al servidor proxy (este campo está disponible si se selecciona la casilla **Autenticación del servidor proxy**).

- **Contraseña**

  Contraseña que especifica el usuario con cuya cuenta se establece la conexión al servidor proxy (este campo está disponible si se selecciona la casilla **Autenticación del servidor proxy**).

  Para ver la contraseña indicada, mantenga presionado el botón **Mostrar** durante la cantidad de tiempo que sea necesario.

Puede configurar el acceso a Internet más tarde, sin usar el asistente de inicio rápido.

## Paso 2. Selección del método de activación de la aplicación

Seleccione una de las siguientes opciones de activación de Kaspersky Security Center:

- **Insertando su código de activación**

  Un *código de activación* es una secuencia única formada por 20 caracteres alfanuméricos. Se ingresa un código de activación para agregar una clave que activa Kaspersky Security Center. Recibe el código de activación en la dirección de correo electrónico que especificó después de comprar Kaspersky Security Center.

  Para activar la aplicación mediante el código de activación, necesita acceso a Internet para establecer la conexión con los servidores de activación de Kaspersky.

  Si seleccionó esta opción de activación, puede activar la opción **Distribuir la clave de licencia automáticamente a los dispositivos administrados**.

  Si esta opción está habilitada, la clave de licencia se distribuirá automáticamente a los dispositivos administrados.

  Si esta opción está desactivada, podrá distribuir la clave de licencia a los dispositivos administrados más adelante en el nodo **Licencias de Kaspersky** del árbol de la Consola de administración.

  Si por algún motivo la activación con el código de activación no se realiza correctamente, puede activar la aplicación mediante un archivo de clave.

- **Especificando un archivo de clave**

  El *archivo de clave* es un archivo con la extensión .key que le proporciona Kaspersky. Los archivos de clave se usan para agregar una clave que activa la aplicación.

  Los métodos para obtener el archivo de clave se describen en la siguiente sección: Acerca del archivo de clave.

  Para activar la aplicación con un archivo de clave, no es necesario conectarse a los servidores de activación de Kaspersky.

  Si seleccionó esta opción de activación, puede activar la opción **Distribuir la clave de licencia automáticamente a los dispositivos administrados**.

  Si esta opción está habilitada, la clave de licencia se distribuirá automáticamente a los dispositivos administrados.

  Si esta opción está desactivada, podrá distribuir la clave de licencia a los dispositivos administrados más adelante en el nodo **Licencias de Kaspersky** del árbol de la Consola de administración.

- **Posponiendo la activación de aplicaciones**

  La aplicación funcionará con una funcionalidad básica, sin Administración de dispositivos móviles y sin Administración de vulnerabilidades y parches.

Si decide posponer la activación de la aplicación, podrá agregar una clave de licencia en cualquier otro momento.

## Paso 3. Selección de las áreas de protección y sistemas operativos

Seleccione las áreas que desee proteger y los sistemas operativos que estén presentes en su red. Cuando selecciona estas opciones, especifica los filtros para los complementos de administración de aplicaciones y los paquetes de distribución en los servidores de Kaspersky que puede descargar para instalar en los dispositivos cliente en su red. Seleccione las opciones:

- **Áreas**

  Puede elegir las siguientes áreas de protección:

  - **Estaciones de trabajo**. Seleccione esta opción si desea proteger las estaciones de trabajo en su red. La estación de trabajo está seleccionada de forma predeterminada.
  - **Servidores de archivos y almacenamiento**. Seleccione esta opción si desea proteger los servidores de archivos en su red.
  - **Dispositivos móviles**. Seleccione esta opción si desea proteger los dispositivos móviles pertenecientes a la empresa o a los empleados de la empresa. Si selecciona esta opción pero no indica una licencia con la función de Administración de dispositivos móviles, aparecerá un mensaje en el que se le solicita que brinde una licencia con la función de Administración de dispositivos móviles. Si no brinda una licencia, no puede utilizar la función de dispositivos móviles.
  - **Virtualización**. Seleccione esta opción si desea proteger las máquinas virtuales en su red.
  - **Kaspersky Antispam**. Seleccione esta opción si desea proteger los servidores de correos electrónicos de su organización contra el correo no deseado, el fraude y la entrega de malware.

- **Sistemas operativos**

  Puede seleccionar las siguientes plataformas:

  - Microsoft Windows
  - Linux
  - macOS
  - Android
  - Otro

  Para obtener información sobre los sistemas operativos compatibles, consulte Requisitos de hardware y software.

Puede seleccionar los paquetes de aplicaciones de Kaspersky de la lista de paquetes disponibles más adelante, sin usar el asistente de inicio rápido. Para simplificar la búsqueda de los paquetes necesarios, puede filtrar la lista de paquetes disponibles por los siguientes criterios:

- Área de protección
- Tipo de software descargado (paquete de distribución, utilidad, complemento o complemento web)

- Versión de la aplicación Kaspersky
- Idioma de localización de la aplicación Kaspersky

## Paso 4. Selección de complementos para las aplicaciones administradas

Seleccione los complementos para aplicaciones administradas que se instalarán. Se muestra una lista de complementos ubicados en los servidores de Kaspersky. La lista se filtra según las opciones que seleccione en el paso anterior del asistente. Por defecto, una lista completa incluye complementos de todos los idiomas. Para mostrar solo el complemento de un idioma específico, seleccione el idioma de la lista desplegable **Mostrar el idioma de localización de la Consola de administración o**. La lista de complementos incluye las siguientes columnas:

- **Nombre de la aplicación**

  Estarán seleccionados los complementos que dependan de los componentes y las plataformas que haya seleccionado en el paso anterior.

- **Versión de la aplicación**

  La lista incluye complementos de todas las versiones colocadas en los servidores de Kaspersky. De forma predeterminada, se seleccionan los complementos de las últimas versiones.

- **Idioma de localización**

  De forma predeterminada, el idioma de localización de un complemento está definido por el idioma de Kaspersky Security Center que ha seleccionado en la instalación. Puede especificar otros idiomas en la lista desplegable **Mostrar el idioma de localización de la Consola de administración o**.

Después de seleccionar los complementos, su instalación comienza automáticamente en una ventana separada. Para instalar algunos complementos, debe aceptar los términos del EULA. Lea el texto de EULA, seleccione la opción **Acepto los términos del Contrato de licencia** y haga clic en el botón **Instalar**. Si no acepta los términos del EULA, el complemento no se instala.

Una vez completada la instalación, cierre la ventana de instalación.

También puede seleccionar los complementos de administración más tarde, sin usar el asistente de inicio rápido.

## Paso 5. Descarga de paquetes de distribución y creación de paquetes de instalación

Kaspersky Endpoint Security para Windows incluye una herramienta de cifrado para la información almacenada en los dispositivos cliente. Para descargar un paquete de distribución de Kaspersky Endpoint Security para Windows válido para las necesidades de su organización, consulte la legislación del país donde se encuentran los dispositivos cliente de su organización.

En la ventana **Tipo de cifrado**, seleccione uno de los siguientes tipos de cifrado:

- Cifrado fuerte (AES256). Este tipo de cifrado utiliza una longitud de clave de 256 bits.
- Cifrado ligero (AES56). Este tipo de cifrado utiliza una longitud de clave de 56 bits.

La ventana **Tipo de cifrado** aparecerá únicamente si ha seleccionado **Estaciones de trabajo** como área de protección y **Microsoft Windows** como plataforma.

Después de seleccionar un tipo de cifrado, se muestra una lista completa de paquetes de distribución de ambos tipos de cifrado. El paquete de distribución que corresponda al tipo de cifrado elegido estará seleccionado en dicha lista. El idioma del paquete de distribución corresponde al idioma de Kaspersky Security Center. Si no existe un paquete de distribución de Kaspersky Endpoint Security para Windows para el idioma de Kaspersky Security Center, se selecciona el paquete de distribución en inglés.

En la lista, puede seleccionar los idiomas del paquete de distribución por medio de la lista desplegable **Mostrar el idioma de localización de la Consola de administración o**.

Los paquetes de distribución de las aplicaciones administradas pueden requerir que la versión de Kaspersky Security Center instalada no sea anterior a una versión en particular.

En la lista, puede seleccionar paquetes de distribución de cualquier tipo de cifrado, diferentes de los que ha seleccionado en la ventana **Tipo de cifrado**. Después de haber seleccionado un paquete de distribución para Kaspersky Endpoint Security para Windows, comienza la descarga de los paquetes de distribución, correspondientes a los componentes y plataformas. Puede controlar el progreso de descarga en la columna **Estado de descarga**. Una vez finalizado el Asistente de inicio rápido, los paquetes de instalación del Agente de red para Windows y de las aplicaciones de Kaspersky administradas se muestran en la lista **Servidor de administración → Avanzado → Instalación remota → Paquetes de instalación**.

Para finalizar la descarga de algunos paquetes de distribución, debe aceptar el EULA. Cuando hace clic en el botón **Aceptar**, se muestra el texto de EULA. Para avanzar al siguiente paso del asistente, debe aceptar los términos y condiciones del EULA y los términos y condiciones de la Política de privacidad de Kaspersky. Seleccione las opciones relacionadas con el EULA y la Política de privacidad de Kaspersky, y haga clic en el botón **Aceptar todos**. Si no acepta los términos y condiciones, se cancela la descarga del paquete.

Después de haber aceptado los términos y condiciones del EULA y los términos y condiciones de la Política de privacidad de Kaspersky, la descarga de los paquetes de distribución continúa. Cuando finaliza la descarga, se muestra el estado **Se creó el paquete de instalación**. Más tarde, podrá usar paquetes de instalación para desplegar las aplicaciones de Kaspersky a los dispositivos cliente.

Puede crear paquetes de instalación manualmente, por separado del asistente de inicio rápido. Vaya a **Servidor de administración → Avanzado → Instalación remota → Paquetes de instalación** en el árbol de la consola de administración.

## Paso 6. Configuración del uso de Kaspersky Security Network

Puede obtener acceso a las bases de datos de reputación de Kaspersky Security Network para garantizar una respuesta rápida de las aplicaciones de Kaspersky ante las amenazas, mejorar la eficacia de algunos componentes de protección y reducir el riesgo de falsos positivos.

Lea la Declaración de KSN que se muestra en la ventana. Especifique la configuración para transmitir la información sobre operaciones Kaspersky Security Center a la base de conocimientos de Kaspersky Security Network. Seleccione una de las siguientes opciones:

- **Acepto utilizar Kaspersky Security Network**

  Kaspersky Security Center y las aplicaciones administradas instaladas en dispositivos cliente transferirán automáticamente su información de operación a Kaspersky Security Network. Participar en Kaspersky Security Network permite que las bases de datos con información sobre virus y otros riesgos se actualicen más rápidamente, lo cual se traduce en una mayor velocidad de respuesta ante amenazas a la seguridad emergentes.

- **No acepto utilizar Kaspersky Security Network**

  Kaspersky Security Center y las aplicaciones administradas no proporcionarán información a Kaspersky Security Network.

  Si selecciona esta opción, se deshabilitará el uso de Kaspersky Security Network.

Si descargó el complemento Kaspersky Endpoint Security para Windows, se muestran las dos declaraciones de KSN: Declaración de KSN para Kaspersky Security Center y Declaración de KSN para Kaspersky Endpoint Security para Windows. Las declaraciones de KSN para otras aplicaciones de Kaspersky administradas, cuyos complementos se descargaron, se muestran en ventanas diferentes y debe aceptar (o rechazar) cada una por separado.

También puede configurar el acceso del Servidor de Administración a Kaspersky Security Network (KSN) más adelante en la ventana de propiedades del Servidor de administración de la Consola de administración.

## Paso 7. Configuración de notificaciones por correo electrónico

Configure el envío de notificaciones sobre eventos registrados durante el funcionamiento de aplicaciones de Kaspersky en los dispositivos administrados. Estos parámetros se usan como la configuración predeterminada para el Servidor de administración.

Para configurar la entrega de notificaciones sobre eventos que ocurren en Aplicaciones de Kaspersky, use la configuración siguiente:

- **Destinatarios (direcciones de correo electrónico)**

  Las direcciones de correo electrónico de usuarios a quien la aplicación enviará notificaciones. Puede ingresar una o más direcciones; si ingresa más de una dirección, sepárelas con un punto y coma.

- **Servidores SMTP**

  La dirección o direcciones de los servidores de correo de su organización.

  Si ingresa más de una dirección, sepárelas con un punto y coma. Puede utilizar los siguientes parámetros:

  - Dirección IPv4 o IPv6
  - Nombre de la red de Windows (nombre NetBIOS) del dispositivo
  - Nombre DNS del servidor SMTP

- **Puerto de los servidores SMTP**

  Número del puerto de comunicación del servidor SMTP. Si utiliza varios servidores SMTP, la conexión con ellos se establecerá a través del puerto de comunicación especificado. El número de puerto predeterminado es 25.

- **Utilizar autenticación ESMTP**

  Habilita la compatibilidad con la autenticación ESMTP. Cuando la casilla está seleccionada, en los campos **Nombre de usuario** y **Contraseña**, puede especificar la configuración de la autorización de ESMTP. Esta casilla no está marcada de manera predeterminada.

- **Configuración**

  Configure los siguientes ajustes:

  - **Asunto** (asunto de un mensaje de correo electrónico)
  - **Dirección de correo electrónico del remitente**
  - **Configuración de TLS para el servidor SMTP**

  Puede especificar la configuración de TLS para el servidor SMTP:

  Puede deshabilitar el uso de TLS, usar TLS si el servidor SMTP admite este protocolo o forzar el uso de TLS únicamente. Si elige usar solo TLS, especifique un certificado para la autenticación del servidor SMTP e indique si desea habilitar la comunicación a través de cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. Además, si elige usar solo TLS, puede especificar un certificado para la autenticación del cliente en el servidor SMTP.

  - Busque un archivo de certificados del servidor SMTP:

  Puede recibir un archivo con la lista de certificados de una autoridad de certificación confiable y cargar el archivo al Servidor de administración. Kaspersky Security Center verifica si el certificado de un servidor SMTP también está firmado por una autoridad de certificación confiable. Si el certificado de un servidor SMTP no se recibe de una autoridad de certificación confiable, Kaspersky Security Center no podrá conectarse al servidor SMTP.

  - Busque un archivo de certificados cliente:

  Puede utilizar un certificado recibido de cualquier fuente (por ejemplo, de una entidad de certificación de confianza). Deberá especificar el certificado y su clave privada. Puede usar, para ello, alguno de los siguientes tipos de certificado:

  - Certificado X-509:

  Especifique el archivo con el certificado y el archivo con la clave privada. Puede cargar estos archivos en cualquier orden. Cuando se cargan ambos archivos, especifique la contraseña para descifrar la clave privada. Si la clave privada no está cifrada, puede dejar la contraseña en blanco.

  - Contenedor pkcs12:

  Debe cargar un solo archivo que contenga el certificado y la clave privada. Cuando se carga el archivo, debe especificar la contraseña para decodificar la clave privada. Si la clave privada no está codificada, puede dejar la contraseña en blanco.

Puede probar la configuración de la notificación por correo electrónico nueva haciendo clic en el botón **Enviar mensaje de prueba**.

También puede configurar notificaciones de eventos más tarde, sin usar el asistente de inicio rápido.

## Paso 8. Configuración de administración de actualizaciones

Ajuste la configuración para administrar las actualizaciones de las aplicaciones instaladas en los dispositivos cliente.

Solo puede configurar estos ajustes si ha proporcionado una clave de licencia con la opción de Administración de vulnerabilidades y parches.

En el grupo de configuraciones **Buscar actualizaciones e instalarlas**, puede seleccionar un modo de búsqueda e instalación de actualizaciones de Kaspersky Security Center:

- **Buscar actualizaciones requeridas**

  La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se creará automáticamente si no existe.

  Esta opción está seleccionada de forma predeterminada.

- **Buscar e instalar actualizaciones requeridas**

  Las tareas *Buscar vulnerabilidades y actualizaciones requeridas* e *Instalar actualizaciones requeridas y reparar vulnerabilidades* se crearán automáticamente si no existen.

En el grupo de configuraciones de **Windows Server Update Services**, puede seleccionar un modo de sincronización de actualizaciones:

- **Usar los orígenes de actualizaciones definidos en la directiva del dominio**

  Los dispositivos cliente descargarán las actualizaciones de Windows Update de conformidad con la configuración de la directiva de su dominio. La directiva del Agente de red se creará automáticamente en caso de que no exista.

- **Usar el Servidor de administración como servidor WSUS**

  Los dispositivos cliente descargarán las actualizaciones de Windows Update del Servidor de administración. La tarea *Sincronización con Windows Update* y la directiva del Agente de red se crean automáticamente si no existen.

Puede crear las tareas *Buscar vulnerabilidades y actualizaciones necesarias* e *Instalar actualizaciones necesarias y corregir vulnerabilidades* por separado desde el asistente de inicio rápido. Para usar el Servidor de administración como servidor de WSUS, debe crear la tarea *Realizar la sincronización de Windows Update* y seleccionar la opción **Usar el Servidor de administración como servidor WSUS** en la directiva del Agente de red.

## Paso 9. Creación de una configuración de protección inicial

La ventana **Configuración inicial de la protección** muestra una lista de directivas y tareas creadas automáticamente. Se crean las siguientes directivas y tareas:

- Directiva del Agente de red de Kaspersky Security Center
- Directivas para aplicaciones de Kaspersky administradas cuyos complementos de administración se instalaron antes
- Tarea Mantenimiento del Servidor de administración
- Tarea Copia de seguridad de los datos del Servidor de administración
- Tarea Descargar actualizaciones en el repositorio del Servidor de administración
- Tarea Buscar vulnerabilidades y actualizaciones requeridas
- Tarea Instalar actualización

Espere a que terminen de crearse las tareas y directivas antes de avanzar al siguiente paso del asistente.

Si ha descargado e instalado el complemento para Kaspersky Endpoint Security para Windows 10 Service Pack 1 y versiones posteriores hasta 11.0.1, durante la creación de directivas y tareas, se abre una ventana para la configuración inicial de la zona de confianza de Kaspersky Endpoint Security para Windows. La aplicación le solicitará agregar proveedores verificados por Kaspersky en la zona de confianza con el fin de excluir sus aplicaciones de los análisis para impedir que se bloqueen por accidente. Puede crear exclusiones recomendadas ahora o crear una lista de exclusiones más adelante. Para hacerlo, seleccione lo siguiente en el árbol de consola: **Directivas** → menú de propiedades de Kaspersky Endpoint Security → **Protección avanzada contra amenazas** → **Zona de confianza** → **Configuración** → **Agregar**. La lista de exclusiones de análisis puede modificarse en cualquier momento al usar la aplicación.

> Las operaciones en la zona de confianza se realizan mediante el uso de herramientas integradas en Kaspersky Endpoint Security para Windows. Si desea obtener instrucciones detalladas sobre cómo realizar estas operaciones, así como una descripción de las funciones de cifrado, consulte la Ayuda en línea de Kaspersky Endpoint Security para Windows.

Para terminar la configuración inicial de la zona de confianza y volver al Asistente, haga clic en **Aceptar**.

Haga clic en **Siguiente**. Este botón se hace disponible después de todas las directivas necesarias y las tareas se han creado.

También puede crear las tareas y directivas requeridas más tarde, sin usar el asistente de inicio rápido.

## Paso 10. Conexión de dispositivos móviles

Si habilitó el área de protección **Dispositivos móviles** en los ajustes del Asistente, especifique los parámetros que se usarán para conectar los dispositivos móviles corporativos de la organización administrada. Si no habilitó el área de protección **Dispositivos móviles**, este paso se omitirá.

En este paso del Asistente, puede hacer lo siguiente:

- Configurar puertos para la conexión de dispositivos móviles
- Configurar la autenticación del Servidor de administración
- Crear o administrar certificados
- Configurar la emisión, la actualización automática y el cifrado de certificados de tipo general
- Crear una regla de movimiento para dispositivos móviles

*Para configurar los puertos que se usarán para la conexión de dispositivos móviles:*

1. Haga clic en el botón **Configurar** a la derecha del campo **Conexión de dispositivos móviles**.
2. En la lista desplegable, seleccione **Configurar puertos**.
   Se abre la ventana de propiedades del Servidor de administración. Vaya a la sección **Puertos adicionales**.

3. En la sección **Puertos adicionales**, configure los ajustes para la conexión de dispositivos móviles:

- **Puerto SSL para el servidor proxy de activación**

  Número del puerto SSL que Kaspersky Endpoint Security para Windows usará para conectarse con los servidores de activación de Kaspersky.

  El número de puerto predeterminado es 17000.

- **Abrir puerto para dispositivos móviles**

  Se abrirá un puerto para que los dispositivos móviles se conecten al Servidor de administración de licencias. Si desea definir el número de puerto y otros ajustes, podrá hacerlo en los campos de abajo.

  Esta opción está activada de forma predeterminada.

- **Puerto para la sincronización de dispositivos móviles**

  Número del puerto que los dispositivos móviles usarán para establecer conexión e intercambiar datos con el Servidor de administración. El número de puerto predeterminado es 13292.

  Puede asignar un puerto diferente si utiliza el puerto 13292 para otros fines.

- **Puerto para la activación de dispositivos móviles**

  Puerto que Kaspersky Endpoint Security para Android usará para conectarse con los servidores de activación de Kaspersky.

  El número de puerto predeterminado es 17100.

- **Abrir puerto para dispositivos con protección de UEFI y dispositivos con KasperskyOS**

  Los dispositivos con protección de UEFI podrán conectarse al Servidor de administración.

- **Puerto para dispositivos con protección de UEFI y dispositivos con KasperskyOS**

  Puede cambiar el número de puerto si la opción **Abrir puerto para dispositivos con protección de UEFI y dispositivos con KasperskyOS** está habilitada. El número de puerto predeterminado es 13294.

- **Abrir puertos para Prometheus**

  El puerto para las solicitudes pull de Prometheus. El número de puerto predeterminado es 13296.

4. Haga clic en **Aceptar** para guardar los cambios y regresar al Asistente de inicio rápido.

Una de sus tareas consiste en configurar el mecanismo por el cual los dispositivos móviles autentican la identidad del Servidor de administración y, de manera inversa, el mecanismo por el cual el Servidor de administración autentica la identidad de los dispositivos móviles. Si lo desea, puede configurar la autenticación en otro momento, por fuera del Asistente de inicio rápido.

*Para configurar la autenticación del Servidor de administración por parte de los dispositivos móviles:*

1. Haga clic en el botón **Configurar** a la derecha del campo **Conexión de dispositivos móviles**.
2. En la lista desplegable, seleccione **Configurar autenticación**.

   Se abre la ventana de propiedades del Servidor de administración y muestra la sección **Certificados**.
3. En el grupo de opciones **Autenticación del Servidor de administración por dispositivos móviles**, seleccione la opción de autenticación para los dispositivos móviles. A continuación, en el grupo de opciones **Autenticación del Servidor de administración por dispositivos con protección de UEFI**, seleccione la opción de autenticación para los dispositivos con protección de UEFI.

   Cuando el Servidor de administración intercambia datos con los dispositivos cliente, se utiliza un certificado para autenticarlo.

   De forma predeterminada, el Servidor de administración usa el certificado que se crea al instalar el Servidor de administración. Si lo desea, puede agregar un nuevo certificado.

*Para agregar un nuevo certificado (opcional):*

1. Seleccione **Otro certificado**.

   Aparece el botón **Examinar**.
2. Haga clic en el botón **Examinar**.

3. En la ventana que se abre, defina los ajustes del certificado:

- Tipo de certificado

  Utilice la lista desplegable para seleccionar un tipo de certificado:

  - **Certificado X.509**Certificado X-509: Si selecciona esta opción, deberá seleccionar la clave privada de un certificado y un certificado abierto:
    - **Clave privada (.prk, .pem)**. Haga clic en el botón **Examinar** de este campo para seleccionar la clave privada de un certificado en formato PKCS #8 (*.prk).
    - **Clave pública (.cer)**. Haga clic en el botón **Examinar** de este campo para seleccionar una clave pública en formato PEM (*.cer).
  - **Contenedor PKCS #12**. Seleccione esta opción si desea elegir un archivo de certificado en formato P12 o PFX. Tras elegir esta opción, haga clic en el botón **Examinar** y complete el campo **Archivo del certificado**.

- Hora de activación:
  - Inmediatamente

    El certificado en uso se reemplazará inmediatamente con el nuevo cuando haga clic en **Aceptar**.

    Los dispositivos móviles conectados antes de esta acción no podrán conectarse al Servidor de administración.

  - Después de que este período caduca, días

    Si selecciona esta opción, se generará un certificado de reserva. El certificado en uso se reemplazará con el nuevo una vez que transcurra el número de días especificado. La fecha de entrada en vigor del certificado de reserva se muestra en la sección **Certificados**.

    Se recomienda planificar la reemisión con antelación suficiente. Los dispositivos móviles deberán descargar el certificado de reserva antes de que caduque el período especificado. Una vez que el certificado vigente se sustituya por el nuevo, los dispositivos móviles conectados antes del cambio no podrán conectarse al Servidor de administración si no tienen el certificado de reserva.

4. Haga clic en el botón **Propiedades** para ver la configuración del certificado del Servidor de administración seleccionado.

*Para volver a emitir un certificado emitido a través del Servidor de administración:*

1. Seleccione **Certificado emitido usando mediante el Servidor de administración**.
2. Haga clic en el botón **Emitir nuevamente**.
3. En la ventana que se abre, defina los siguientes ajustes:

- Dirección de conexión:
  - Usar la dirección de conexión antigua

Los dispositivos móviles seguirán usando la misma dirección para conectarse al Servidor de administración.

Esta opción está seleccionada de forma predeterminada.

- Cambiar la dirección de la conexión a

  Si desea que los dispositivos móviles se conecten a una dirección diferente, introduzca la nueva dirección en este campo.

  Cuando se modifica la dirección a la que se conectan los dispositivos móviles, se vuelve necesario emitir un nuevo certificado. El certificado antiguo pierde validez en todos los dispositivos móviles conectados. Los dispositivos conectados antes del cambio pierden la capacidad de conectarse al Servidor de administración y se convierten en dispositivos no administrados.

- Hora de activación:

  - Inmediatamente

    El certificado en uso se reemplazará inmediatamente con el nuevo cuando haga clic en **Aceptar**.

    Los dispositivos móviles conectados antes de esta acción no podrán conectarse al Servidor de administración.

  - Después de que este período caduca, días

    Si selecciona esta opción, se generará un certificado de reserva. El certificado en uso se reemplazará con el nuevo una vez que transcurra el número de días especificado. La fecha de entrada en vigor del certificado de reserva se muestra en la sección **Certificados**.

    Se recomienda planificar la reemisión con antelación suficiente. Los dispositivos móviles deberán descargar el certificado de reserva antes de que caduque el período especificado. Una vez que el certificado vigente se sustituya por el nuevo, los dispositivos móviles conectados antes del cambio no podrán conectarse al Servidor de administración si no tienen el certificado de reserva.

4. Haga clic en **Aceptar** para guardar los cambios y regresar a la ventana **Certificados**.

5. Haga clic en **Aceptar** para guardar los cambios y regresar al Asistente de inicio rápido.

*Para configurar la emisión, la actualización automática y el cifrado de los certificados de tipo general con los que el Servidor de administración identifica los dispositivos móviles:*

1. Haga clic en el botón **Configurar** a la derecha del campo **Autenticación de dispositivos móviles**.

   Se abre la ventana **Reglas de emisión de certificados** en la sección **Emisión de certificados para dispositivos móviles**.

2. De ser necesario, configure los siguientes ajustes en la sección **Configuración de emisión**:

   - **Vigencia del certificado, días**

     Vigencia del certificado en días. La vigencia predeterminada de un certificado es de 365 días. Una vez que caduca este período, los dispositivos móviles pierden la capacidad de conectarse al Servidor de administración.

   - **Origen del certificado**

     Indique de dónde provienen los certificados de tipo general que se utilizan para los dispositivos móviles. Los certificados pueden ser emitidos por el Servidor de administración o pueden seleccionarse manualmente.

   Si ha configurado la integración con una infraestructura de claves públicas (PKI) en la sección **Integración con PKI**, puede modificar las plantillas de certificados. Para tal fin, tiene acceso a los siguientes campos, que permiten seleccionar la plantilla:

   - **Plantilla predeterminada**

     Seleccione esta opción para usar un certificado emitido por una entidad de certificación externa con la plantilla predeterminada.

     Esta opción está seleccionada de forma predeterminada.

   - **Otra plantilla**

     Seleccione esta opción para elegir una plantilla usada para emitir certificados. Puede especificar plantillas de certificados en el dominio. El botón **Actualizar lista** actualiza la lista de plantillas de certificados.

3. De ser necesario, configure los siguientes ajustes relativos a la emisión automática de certificados en la sección **Configuración de actualización automática**:

   - Renovar cuando el certificado caduque en (días)

     Antelación con la que el Servidor de administración emitirá un nuevo certificado cuando el certificado vigente esté próximo a caducar. Si el valor del campo es 4, por ejemplo, el Servidor de administración emitirá un nuevo certificado cuatro días antes de que caduque el certificado vigente. El valor predeterminado es 7.

   - Volver a emitir certificados automáticamente si es posible

     Seleccione esta opción para que el nuevo certificado se emita automáticamente al llegar el número de días indicado en el campo **Renovar cuando el certificado caduque en (días)**. Si el certificado vigente se emitió de manera manual, no se lo podrá renovar automáticamente; en ese caso, habilitar esta opción no tendrá ningún efecto.

     Esta opción está deshabilitada de forma predeterminada.

   Los certificados son reemitidos automáticamente por una entidad de certificación.

4. De ser necesario, en la sección **Protección con contraseña**, defina los ajustes para descifrar certificados durante la instalación.

   Seleccione la opción **Solicitar contraseña durante la instalación de certificados** para que se le solicite al usuario la contraseña cuando el certificado se instale en un dispositivo móvil. La contraseña solo se utiliza una vez, durante la instalación del certificado en el dispositivo móvil.

   La contraseña será generada por el Servidor de administración automáticamente y se enviará a la dirección de correo electrónico que se ingrese. Ingrese su propia dirección de correo electrónico si quiere ocuparse de brindarle la contraseña al usuario; de lo contrario, puede usar la dirección de correo electrónico del usuario.

   Puede usar el control deslizante para especificar el número de caracteres de la contraseña de descifrado del certificado.

   La opción de solicitar la contraseña se requiere, por ejemplo, para proteger un certificado compartido en un paquete de instalación independiente de Kaspersky Endpoint Security para Android. Si un intruso roba el paquete de instalación independiente publicado en el Servidor web de Kaspersky Security Center, la protección con contraseña le impedirá acceder al certificado compartido.

   Cuando esta opción se encuentra deshabilitada, el certificado se descifra automáticamente durante la instalación y no se le pide al usuario que ingrese una contraseña. Esta opción está deshabilitada de forma predeterminada.

5. Haga clic en **Aceptar** para guardar los cambios y regresar a la ventana del Asistente de inicio rápido.

   Haga clic en el botón **Cancelar** para volver al Asistente de inicio rápido sin guardar los cambios realizados.

*Para habilitar la función que mueve los dispositivos móviles a un grupo de administración a elección:*

En el campo **Reglas para mover dispositivos móviles automáticamente**, seleccione la opción **Crear una regla de movimiento para dispositivos móviles**.

Cuando seleccione la opción **Crear una regla de movimiento para dispositivos móviles**, la aplicación creará automáticamente una regla de movimiento para trasladar los siguientes dispositivos con Android y iOS al grupo **Dispositivos administrados**:

- Dispositivos con sistemas operativos Android que tengan instalado un certificado para dispositivos móviles y una copia de Kaspersky Endpoint Security para Android
- Dispositivos con sistemas operativos iOS que tengan instalado un perfil de MDM para iOS con un certificado compartido

Si la aplicación detecta que ya existe una regla de movimiento con estos criterios, no la volverá a crear.

Esta opción está deshabilitada de forma predeterminada.

Kaspersky ha discontinuado Kaspersky Safe Browser.

## Paso 11. Descargar actualizaciones

Las actualizaciones de las bases de datos antivirus para Kaspersky Security Center y las aplicaciones administradas de Kaspersky se descargan automáticamente. Las actualizaciones se descargan de los servidores de Kaspersky.

Para descargar actualizaciones por separado del asistente de inicio rápido, cree y configure la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*.

## Paso 12. Descubrimiento de dispositivos

La ventana **Sondeo de red** muestra la información sobre el estado del sondeo de la red realizada por el Servidor de administración.

Puede ver dispositivos de la red detectados por el Servidor de administración y recibir la ayuda en el funcionamiento con la ventana **Descubrimiento de dispositivos** haciendo clic en los enlaces en la parte inferior de la ventana.

Puede sondear su red más tarde, independientemente del asistente de inicio rápido. Utilice la Consola de administración para configurar el sondeo de Dominios de Windows, Active Directory, rangos de IP y redes IPv6.

## Paso 13. Cierre del asistente de inicio rápido

En la ventana de finalización del Asistente de inicio rápido, seleccione la opción **Ejecutar el Asistente de instalación remota** si desea iniciar la instalación automática de aplicaciones antivirus y/o el Agente de red en dispositivos en su red.

Para finalizar el Asistente, haga clic en el botón **Finalizar**.

# Configuración de la conexión de la Consola de administración al Servidor de administración

La Consola de administración está conectada al Servidor de administración a través del puerto SSL TCP 13291. Los objetos de automatización klakaut pueden utilizar este mismo puerto.

El puerto TCP 14000 se puede utilizar para conectar la Consola de administración, los puntos de distribución, los Servidores de administración secundarios y los objetos de automatización klakaut, así como para recibir datos desde dispositivos cliente.

Normalmente, el puerto SSL TCP 13000 solo puede ser utilizado por el Agente de red, un Servidor de administración secundario y el Servidor de administración principal en DMZ. En algunos casos, es posible que la Consola de administración deba conectarse mediante el puerto SSL 13000:

- Si se prefiere usar un solo puerto SSL tanto para la Consola de administración como para otras actividades (recepción de datos desde dispositivos cliente, conexión de puntos de distribución o conexión de Servidores de administración secundarios).
- Si un objeto de automatización klakaut no se conecta al Servidor de administración directamente, sino mediante un punto de distribución en DMZ.

*Para permitir la conexión de Consola de administración mediante el puerto 13000:*

1. Abra el registro del sistema del dispositivo en el que está instalado el Servidor de administración (por ejemplo, de forma local con el comando regedit en el menú **Iniciar** → **Ejecutar**).
2. Vaya al siguiente archivo:
   - Para sistemas de 32 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - Para sistemas de 64 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. Para la clave LP_ConsoleMustUsePort13291 (DWORD), configure 00000000 como el valor.

   El valor predeterminado especificado para esta clave es 1.
4. Reinicie el servicio del Servidor de administración.

Ahora podrá conectar la Consola de administración al Servidor de administración mediante el puerto 13000.

# Configuración de las opciones de acceso a Internet para el Servidor de administración

Debe configurar el acceso a Internet para usar Kaspersky Security Network y descargar actualizaciones y bases de datos antivirus para Kaspersky Security Center y las aplicaciones de Kaspersky administradas.

*Para especificar la configuración de acceso a Internet para el Servidor de administración:*

1. En el árbol de consola, seleccione el nodo **Servidor de administración %s**.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
3. En la ventana de propiedades del Servidor de administración, vaya a **Avanzado → Configuración de acceso a Internet**.
4. Seleccione la opción **Usar servidor proxy** si desea usar un servidor proxy al conectarse a Internet. Si se selecciona esta opción, los campos estarán disponibles para escribir la configuración. Deberá introducir los siguientes valores de conexión del servidor proxy:

   - **Dirección**

     Dirección del servidor proxy usado para conectar Kaspersky Security Center con Internet.

   - **Número de puerto**

     Número del puerto a través del cual se establecerá la conexión proxy de Kaspersky Security Center.

   - **No usar el servidor proxy para direcciones locales**

     Ningún servidor proxy se usará para conectarse a los dispositivos en la red local.

   - **Autenticación del servidor proxy**

     Si se selecciona esta casilla, en los campos de entrada se podrán especificar las credenciales para la autenticación del servidor proxy.

     Este campo de entrada está disponible cuando la casilla **Usar servidor proxy** está desmarcada.

   - **Nombre de usuario**

     Cuenta de usuario con la que se establece la conexión al servidor proxy (este campo está disponible si se selecciona la casilla **Autenticación del servidor proxy**).

   - **Contraseña**

     Contraseña que especifica el usuario con cuya cuenta se establece la conexión al servidor proxy (este campo está disponible si se selecciona la casilla **Autenticación del servidor proxy**).

     Para ver la contraseña indicada, mantenga presionado el botón **Mostrar** durante la cantidad de tiempo que sea necesario.

También puede configurar el acceso a Internet mediante el asistente de inicio rápido.

# Conexión de dispositivos fuera de la oficina

En esta sección se explica cómo conectar dispositivos fuera de la oficina (es decir, dispositivos administrados que se encuentran fuera de la red principal) al Servidor de administración.

## Escenario: conexión de dispositivos fuera de la oficina mediante una puerta de enlace de conexión

Este escenario describe cómo conectar dispositivos administrados que se encuentran fuera de la red principal al Servidor de administración.

### Requisitos previos

El escenario tiene los siguientes requisitos previos:

- Existe una zona desmilitarizada (DMZ) en la red de su organización.
- El Servidor de administración de Kaspersky Security Center se despliega en la red corporativa.

### Etapas

Este escenario se divide en etapas:

1. **Seleccionar un dispositivo cliente en la DMZ**

   El dispositivo actuará como puerta de enlace de conexión. El dispositivo debe reunir los requisitos para puertas de enlace de conexión.

2. **Instalar el Agente de red en el rol de puerta de enlace de conexión**

   Recomendamos instalar el Agente de red en forma local en el dispositivo elegido.

   De forma predeterminada, el archivo de instalación se encuentra en \\<nombre del servidor>\KLSHARE\PkgInst\NetAgent_<número de versión>.

   En la ventana **Puerta de enlace de conexión** del Asistente de instalación del Agente de red, seleccione **Usar el Agente de red como una puerta de enlace de conexión en la DMZ**. Este modo activa simultáneamente la función de puerta de enlace de conexión y le indica al Agente de red que espere las conexiones del Servidor de administración en lugar de establecer conexiones con el Servidor de administración.

   De forma alternativa, puede instalar el Agente de red en un dispositivo Linux y configurar el Agente de red para que funcione como puerta de enlace de conexión, pero ponga atención a la lista de limitaciones del Agente de red que se ejecuta en los dispositivos Linux.

3. **Permitir las conexiones a la puerta de enlace en los distintos firewalls**

   Para asegurarse de que el Servidor de administración pueda realmente conectarse a la puerta de enlace de conexión en la DMZ, permita conexiones al puerto TCP 13000 en todos los firewalls entre el Servidor de administración y la puerta de enlace de conexión.

   Si la puerta de enlace de conexión no tiene una dirección IP real en Internet, sino que se encuentra detrás de la traducción de direcciones de red (NAT), configure una regla para reenviar las conexiones a través de la NAT.

### 4 Crear un grupo de administración para dispositivos externos

Cree un nuevo grupo dentro del grupo **Dispositivos administrados**. El nuevo grupo albergará los dispositivos externos administrados.

### 5 Conectar la puerta de enlace de conexión al Servidor de administración

La puerta de enlace de conexión que configuró está esperando una conexión del Servidor de administración. El Servidor de administración, sin embargo, no incluye el dispositivo con la puerta de enlace de conexión entre los dispositivos administrados. Esto se debe a que la puerta de enlace no ha intentado conectarse con el Servidor de administración. El problema puede resolverse con un procedimiento especial, que obliga al Servidor de administración a conectarse con la puerta de enlace de conexión.

Haga lo siguiente:

1. Agregue la puerta de enlace de conexión como punto de distribución.
2. Mueva la puerta de enlace de conexión del grupo de **Dispositivos no asignados** al grupo que creó para dispositivos externos.

La puerta de enlace de conexión está conectada y configurada.

### 6 Conectar dispositivos de escritorio externos al Servidor de administración

Por lo general, los dispositivos de escritorio externos no se mueven dentro del perímetro. Por lo tanto, debe configurarlas para que se conecten al Servidor de administración a través de la puerta de enlace durante la instalación del Agente de red.

### 7 Configurar el mecanismo de actualización para los dispositivos de escritorio externos

Si las actualizaciones de las aplicaciones de seguridad están configuradas para descargarse del Servidor de administración, los dispositivos externos descargan las actualizaciones a través de la puerta de enlace de conexión. Esto conlleva dos desventajas:

- El tráfico de Internet generado ocupa ancho de banda innecesariamente.
- Esta no es necesariamente la forma más rápida de obtener actualizaciones. Muy probablemente, lo más rápido y económico sea que los dispositivos externos obtengan las actualizaciones de los servidores de actualizaciones de Kaspersky.

Haga lo siguiente:

1. Mueva todos los dispositivos externos al grupo de administración independiente que creó anteriormente.
2. Asegúrese de que el grupo de dispositivos externos quede excluido de la tarea de actualización.
3. Cree una tarea de actualización separada para el grupo con dispositivos externos.

### 8 Conectar las computadoras portátiles de quienes viajan al Servidor de administración

Las computadoras portátiles de quienes viajan a veces están dentro de la red y, en otras ocasiones, afuera. Para una administración eficaz, debe conectarlas al Servidor de administración de forma diferente según su ubicación. Para un uso eficiente del tráfico, también necesitan recibir actualizaciones de diferentes fuentes según su ubicación.

Necesita configurar reglas para usuarios fuera de la oficina: perfiles de conexión y descripciones de ubicación de red. Cada regla define la instancia del Servidor de administración al que deben conectarse las computadoras portátiles que viajan, según su ubicación y la instancia del Servidor de administración desde el cual deben recibir actualizaciones.

# Escenario: Conectar dispositivos fuera de la oficina mediante un Servidor de administración secundario en la DMZ

Si desea conectar dispositivos administrados que estén fuera de la red principal al Servidor de Administración, puede hacerlo mediante un Servidor de Administración secundario que se encuentre en la zona desmilitarizada (DMZ).

## Requisitos previos

Antes de comenzar, compruebe que hizo lo siguiente:

- Existe una zona desmilitarizada (DMZ) en la red de su organización.
- El Servidor de administración de Kaspersky Security Center queda desplegado en la red corporativa.

## Etapas

Este escenario se divide en etapas:

1. **Seleccionar un dispositivo cliente en la DMZ**

   En la DMZ, seleccione un dispositivo cliente que se utilizará como puerta de enlace de conexión.

2. **Instalar el Servidor de administración de Kaspersky Security Center**

   Para instalar el Servidor de administración de Kaspersky Security Center en este dispositivo local.

3. **Crear una jerarquía de Servidores de administración**

   Si coloca un Servidor de administración secundario en la DMZ, éste debe recibir una conexión proveniente del Servidor de Administración primario. Puede agregar un nuevo Servidor de administración como secundario para que el Servidor de administración principal se conecte al Servidor de administración secundario a través del puerto 13000. Al combinar dos Servidores de administración en una jerarquía, asegúrese de que el puerto 13291 esté accesible en ambos Servidores de administración. La Consola de administración se conecta al Servidor de administración a través del puerto 13291.

4. **Conexión de los dispositivos fuera de la oficina con el Servidor de administración secundario**

   Puede conectar dispositivos que estén fuera de la oficina al Servidor de administración en la DMZ de la misma manera en que se conecta el Servidor de administración y los dispositivos administrados que se encuentran en la red principal. Los dispositivos administrados fuera de la oficina inician la conexión a través del puerto 13000.

# Acerca de la conexión de dispositivos fuera de la oficina

Algunos dispositivos administrados siempre se encuentran fuera de la red principal (por ejemplo, los dispositivos en las sucursales regionales de una empresa; los quioscos, los cajeros automáticos y las terminales instaladas en diversos puntos de venta; dispositivos en las oficinas domésticas de los empleados). Algunos dispositivos se mueven hacia fuera del perímetro de vez en cuando (por ejemplo, las computadoras portátiles de usuarios que visitan sucursales regionales o la oficina de un cliente).

Aún necesita monitorear y administrar la protección de los dispositivos fuera de la oficina, recibir información real sobre su estado de protección y mantener las aplicaciones de seguridad en ellos en el estado actualizado. Esto es necesario porque, por ejemplo, si un dispositivo de este tipo se ve comprometido mientras está lejos de la red principal, podría convertirse en una plataforma para propagar amenazas tan pronto como se conecte a la red principal. Para conectar dispositivos fuera de la oficina al Servidor de administración, puede utilizar los dos métodos siguientes:

- Una puerta de enlace de conexión en la zona desmilitarizada (DMZ)

  Consulte el esquema de tráfico de datos: Servidor de administración en una LAN, dispositivos administrados en Internet, puerta de enlace de conexión en uso

- Un Servidor de administración en DMZ

  Consulte el esquema de tráfico de datos: Servidor de administración en una DMZ, dispositivos administrados en Internet

## Una puerta de enlace de conexión en la DMZ

Un método recomendado para conectar al Servidor de administración dispositivos que están fuera de la oficina consiste en preparar una DMZ en la red de la organización e instalar una puerta de enlace de conexión en la DMZ. Los dispositivos externos se conectarán a la puerta de enlace de conexión, y el Servidor de administración dentro de la red iniciará la conexión con los dispositivos a través de la puerta de enlace de conexión.

En comparación con el otro método, este es más seguro por los siguientes motivos:

- No es necesario abrir el acceso al Servidor de administración desde fuera de la red.

- Una puerta de enlace de conexión comprometida no representa un riesgo elevado para la seguridad de los dispositivos de red. En realidad, una puerta de enlace de conexión no administra ningún elemento por sí misma y no establece ninguna conexión.

Además, una puerta de enlace de conexión no necesita muchos recursos de hardware.

Sin embargo, este método implica un proceso de configuración más complejo:

- Para que un dispositivo funcione como una puerta de enlace de conexión en la DMZ, debe instalar el Agente de red y conectarlo al Servidor de administración de una forma muy concreta.

- No podrá utilizar la misma dirección para conectarse al Servidor de administración en todas las situaciones. Desde fuera del perímetro, deberá emplear no solo una dirección diferente (la dirección de la puerta de enlace de conexión), sino también un modo de conexión diferente: a través de una puerta de enlace de conexión.

- También debe definir una configuración de conexión diferente para las computadoras portátiles que se encuentren en diferentes ubicaciones.

*Para agregar una puerta de enlace de conexión a una red ya configurada:*

1. Instale el Agente de red en el modo de puerta de enlace de conexión.

2. Vuelva a instalar el Agente de red en los dispositivos que desee conectar a la puerta de enlace de conexión recién agregada.

### Un Servidor de administración en la DMZ

Otro método consiste en instalar un único Servidor de administración en la DMZ.

Esta configuración es menos segura que el método anterior. En este caso, para administrar computadoras portátiles externas, el Servidor de administración debe aceptar conexiones desde cualquier dirección de Internet. Continuará administrando todos los dispositivos de la red interna, pero desde la DMZ. Por lo tanto, un Servidor comprometido podría hacer mucho daño, a pesar de la baja probabilidad de que tal evento ocurra.

El riesgo se reduce significativamente si el Servidor de administración en la DMZ no administra dispositivos en la red interna. Por ejemplo, un proveedor de servicios puede utilizar una configuración de este tipo para administrar los dispositivos de los clientes.

Es posible que desee utilizar este método en los siguientes casos:

- Si está familiarizado con la instalación y configuración del Servidor de administración y no desea realizar otro procedimiento para instalar y configurar una puerta de enlace de conexión.
- Si necesita administrar más dispositivos. La capacidad máxima que admite el Servidor de administración es de 100 000 dispositivos, mientras que una puerta de enlace de conexión puede admitir hasta 10 000 dispositivos.

Esta solución también acarrea algunas posibles dificultades:

- El Servidor de administración necesita una base de datos más y más recursos de hardware.
- La información sobre los dispositivos se almacenará en dos bases de datos no relacionadas (una para el Servidor de administración dentro de la red y otra en la DMZ), lo que complica la supervisión.
- Para administrar todos los dispositivos, el Servidor de administración debe estar asociado en una jerarquía, lo que dificulta no solo la supervisión, sino también la administración. Una instancia del Servidor de administración secundario impone limitaciones en las posibles estructuras de los grupos de administración. Debe decidir de qué manera y qué tareas y directivas distribuirá a una instancia del Servidor de administración secundario.
- Configurar dispositivos externos para utilizar el Servidor de administración en la DMZ de forma externa y utilizar el Servidor de administración principal de forma local no es más simple que configurarlos para utilizar una conexión condicional mediante una puerta de enlace.
- Riesgos de seguridad elevados. Si hay una instancia del Servidor de administración comprometida, es más fácil que sus computadoras portátiles administradas se vean comprometidas. Si esto sucede, los hackers solo deben esperar a que una de las computadoras portátiles vuelva a conectarse a la red corporativa para poder continuar con su ataque en la red de área local.

## Conectar dispositivos de escritorio externos al Servidor de administración

Los dispositivos de escritorio que siempre se encuentran fuera de la red principal (por ejemplo, los dispositivos en las sucursales regionales de la empresa, los cajeros automáticos y los dispositivos ubicados en los hogares de los empleados, en los puntos de venta o en las sucursales de la empresa) no se pueden conectar al Servidor de administración en forma directa. Deben hacerlo, en cambio, a través de una puerta de enlace de conexión instalada en la zona desmilitarizada (DMZ). Esta configuración se realiza al instalar el Agente de red en esos dispositivos.

*Para conectar dispositivos de escritorio externos al Servidor de administración:*

1. Cree un paquete de instalación nuevo para el Agente de red.
2. Abra las propiedades del paquete de instalación creado y vaya a la sección **Avanzado**; luego, seleccione la opción **Conectarse al Servidor de administración mediante una puerta de enlace de conexión**.

   La opción **Conectarse al Servidor de administración mediante una puerta de enlace de conexión** no es compatible con la opción **Usar el Agente de red como una puerta de enlace de conexión en la DMZ**. No puede habilitar estas dos configuraciones al mismo tiempo.

3. En **Dirección de puerta de enlace de conexión**, especifique la dirección pública de la puerta de enlace de conexión.

   Si la puerta de enlace de conexión se encuentra detrás de la traducción de direcciones de red (NAT) y no tiene su propia dirección pública, configure una regla de puerta de enlace NAT para reenviar conexiones desde la dirección pública a la dirección interna de la puerta de enlace de conexión.

4. Cree un paquete de instalación independiente basado en el paquete de instalación creado.
5. Entregue el paquete de instalación independiente a los dispositivos de destino. Puede usar para ello una unidad extraíble u otro medio electrónico.
6. Instale el Agente de red desde el paquete independiente.

Los dispositivos de escritorio externos se conectan al Servidor de administración.

## Acerca de los perfiles de conexión para los usuarios fuera de la oficina

Los usuarios de computadoras portátiles fuera de la oficina (más adelante también llamadas "dispositivos") tal vez tengan que cambiar el método de conexión a un Servidor de administración o entre Servidores de administración, según la ubicación actual del dispositivo en la red de la empresa.

Los perfiles de conexión solo son compatibles con dispositivos que ejecutan Windows y MacOS.

### Utilización de direcciones diferentes de un Servidor de administración solo

Los dispositivos con Agente de red instalado pueden conectarse al Servidor de administración desde la red interna de la organización o desde Internet. Esta situación puede requerir que el Agente de red use direcciones diferentes para la conexión con el Servidor de administración: dirección externa del Servidor de administración para conexión a Internet y dirección interna del Servidor de administración para la conexión a la red interna.

Para hacer esto, debe agregar un perfil (para la conexión con el Servidor de administración desde Internet) a la directiva del Agente de red. Añada el perfil en las propiedades de la directiva (sección **Conectividad**, subsección **Perfiles de conexión**). En la ventana de creación de perfil, debe deshabilitar la opción **Usar para recibir actualizaciones solamente** y seleccionar la opción **Sincronizar configuración de conexión con la configuración del Servidor de administración especificada en este perfil**. Si usa una puerta de enlace de conexión para acceder al Servidor de administración (por ejemplo, en una configuración de Kaspersky Security Center como la que se describe en Acceso a Internet: Agente de red como puerta de enlace de conexión en una DMZ), debe especificar la dirección de la puerta de enlace de conexión en el campo correspondiente del perfil de conexión.

### Conmutación entre Servidores de administración según la red actual

Si la organización tiene varias oficinas con Servidores de administración diferentes y algunos dispositivos con Agentes de red instalados se transfieren entre ellos, necesita un Agente de red para conectarse al Servidor de administración de la red local en la oficina donde el dispositivo se localiza actualmente.

En este caso, debe crear un perfil para la conexión con el Servidor de administración en las propiedades de la directiva del Agente de red para cada una de las oficinas, excepto la oficina local donde el Servidor de administración doméstico se encuentra localizado. Debe especificar las direcciones de los Servidores de administración en perfiles de conexión y habilitar o deshabilitar la opción **Usar para recibir actualizaciones solamente**:

- Habilite la opción si necesita que el Agente de red se sincronice con el Servidor de administración doméstico mientras usa el Servidor local para descargar actualizaciones únicamente.
- Deshabilite la opción si es necesario para que el Agente de red sea administrado completamente por el Servidor de administración local.

Después de esto, debe configurar las condiciones de conmutación para los perfiles recién creados: al menos una condición para cada una de las oficinas, excepto la oficina local. El propósito de cada condición consiste en la detección de elementos que son específicos para el entorno de la red de una oficina. Si una condición es verdadera, el perfil correspondiente se activa. Si ninguna de las condiciones es verdadera, el Agente de red cambia al Servidor de administración doméstico.

## Creación de un perfil de conexión para usuarios fuera de la oficina

Los perfiles para establecer conexión con un Servidor de administración solo están disponibles para dispositivos con Windows y macOS.

*Para crear un perfil para la conexión del Agente de red con el Servidor de administración para usuarios fuera de la oficina, haga lo siguiente:*

1. En el árbol de consola, seleccione el grupo de administración para los dispositivos cliente para los que necesita crear un perfil para conectar el Agente de red al Servidor de administración.
2. Realice una de las siguientes acciones:
   - Si desea crear un perfil de conexión para todos los dispositivos del grupo, seleccione una directiva para el Agente de red en el espacio de trabajo, en la pestaña **Directivas**. Abra la ventana de propiedades de la directiva seleccionada.
   - Si desea crear un perfil de conexión para un dispositivo en un grupo, seleccione el dispositivo en el espacio de trabajo del grupo, en la pestaña **Dispositivos**, y realice las siguientes acciones:
     a. Abra la ventana de propiedades del dispositivo seleccionado.
     b. En la sección **Aplicaciones** de la ventana de propiedades del dispositivo seleccione Agente de red.
     c. Abra la ventana de propiedades del Agente de red.
3. En la ventana de propiedades, en la sección **Conectividad** seleccione la subsección **Perfiles de conexión**.

4. En el grupo de configuración **Perfiles de conexión al Servidor de administración**, haga clic en el botón **Agregar**.

   De forma predeterminada, la lista de perfiles de conexión contiene los perfiles <Modo sin conexión> y <Servidor de administración doméstico>. Los perfiles no pueden ser modificados o eliminados.

   El perfil <Modo sin conexión> no especifica ningún Servidor para la conexión. En consecuencia, cuando pasa a operar con este perfil, el Agente de red no intenta conectarse a ningún Servidor de administración y las aplicaciones instaladas en los dispositivos cliente quedan sujetas a directivas de trabajo fuera de la oficina. El perfil <Modo sin conexión> puede ser utilizado si los dispositivos están desconectados de la red.

   El perfil <Servidor de administración doméstico> se utiliza para establecer conexión con el Servidor de administración seleccionado durante la instalación del Agente de red. El perfil <Servidor de administración doméstico> se aplica cuando un dispositivo se conecta de nuevo al Servidor de administración doméstico después de haberse ejecutado en una red externa durante algún tiempo.

5. En la ventana **Perfil nuevo** que se abre, configure el perfil de conexión:

- Nombre del perfil

  En el campo de entrada, puede ver o modificar el nombre del perfil de conexión.

- Servidor de administración

  La dirección del Servidor de administración a la que debe conectarse el dispositivo cliente al activarse el perfil.

- Puerto

  Número de puerto que se utilizará para la conexión.

- Puerto SSL

  Número de puerto para la conexión si se utiliza el protocolo SSL.

- Usar SSL

  Si se habilita esta opción, la conexión se establece a través un puerto seguro mediante el protocolo SSL.

  Esta opción está activada de forma predeterminada. Recomendamos no deshabilitar esta opción; de lo contrario, la conexión quedará desprotegida.

- Haga clic en el enlace **Configurar conexión mediante servidor proxy** para configurar la conexión a través de un servidor proxy. Seleccione la opción **Usar servidor proxy** si desea usar un servidor proxy al conectarse a Internet. Si selecciona esta opción, se habilitarán campos para que configure los ajustes pertinentes. Deberá introducir los siguientes valores de conexión del servidor proxy:

  - Dirección del servidor proxy

    Dirección del servidor proxy usado para conectar Kaspersky Security Center con Internet.

  - Número de puerto

    Número del puerto a través del cual se establecerá la conexión proxy de Kaspersky Security Center.

  - Autenticación del servidor proxy

    Si se selecciona esta casilla, en los campos de entrada se podrán especificar las credenciales para la autenticación del servidor proxy.

    Este campo de entrada está disponible cuando la casilla **Usar servidor proxy** está desmarcada.

  - Nombre de usuario (este campo está disponible si se selecciona la opción **Autenticación del servidor proxy**)

Cuenta de usuario con la que se establece la conexión al servidor proxy (este campo está disponible si se selecciona la casilla **Autenticación del servidor proxy**).

- **Contraseña** (este campo está disponible si se selecciona la opción **Autenticación del servidor proxy**)

  Contraseña que especifica el usuario con cuya cuenta se establece la conexión al servidor proxy (este campo está disponible si se selecciona la casilla **Autenticación del servidor proxy**).

  Para ver la contraseña indicada, mantenga presionado el botón **Mostrar** durante la cantidad de tiempo que sea necesario.

- **Parámetros de la puerta de enlace de conexión**

  La dirección de la puerta de enlace a través de la cual los dispositivos cliente se conectan al Servidor de administración.

- **Habilitar el modo fuera de la oficina**

  Si se habilita esta opción, en caso de que se establezca la conexión mediante este perfil, las aplicaciones instaladas en el dispositivo cliente utilizarán perfiles de directiva para dispositivos en modo fuera de la oficina, así como directivas para fuera de la oficina. Si no hay una directiva fuera de la oficina definida para la aplicación, se utilizará la directiva activa.

  Si se deshabilita esta opción, las aplicaciones utilizarán directivas activas.

  Esta opción está deshabilitada de forma predeterminada.

- **Usar para recibir actualizaciones solamente**

  Si se habilita esta opción, el perfil se utilizará solamente para que las aplicaciones instaladas en el dispositivo cliente descarguen actualizaciones. Para otras operaciones, la conexión al Servidor de administración será establecida con los parámetros de conexión iniciales definidos durante la instalación del Agente de red.

  Esta opción está activada de forma predeterminada.

- **Sincronizar configuración de conexión con la configuración del Servidor de administración especificada en este perfil**

  Si se habilita esta opción, el Agente de red se conectará al Servidor de administración usando la configuración especificada en las propiedades del perfil.

  Si se deshabilita esta opción, el Agente de red se conectará al Servidor de administración usando la configuración original especificada durante la instalación.

  Esta opción está disponible si se deshabilita la opción **Usar para recibir actualizaciones solamente**.

  Esta opción está deshabilitada de forma predeterminada.

6. Seleccione la opción **Habilitar el modo fuera de la oficina cuando el Servidor de administración no esté disponible** para permitir que las aplicaciones instaladas en un dispositivo cliente usen perfiles de directiva para dispositivos en modo fuera de la oficina, así como directivas para fuera de la oficina, en cualquier intento de conexión si el Servidor de administración no está disponible. Si no hay una directiva fuera de la oficina definida para la aplicación, se utilizará la directiva activa.

Se creará un perfil para la conexión del Agente de red con el Servidor de administración para usuarios fuera de la oficina. Cuando el Agente de red se conecte al Servidor de administración con el nuevo perfil, las aplicaciones instaladas en el dispositivo cliente quedarán sujetas a directivas para dispositivos en modo fuera de la oficina o directivas para fuera de la oficina.

## Acerca de cambiar el Agente de red a otros Servidores de administración

La configuración inicial de la conexión del Agente de red al Servidor de administración se define durante la instalación del Agente de red. Para cambiar el Agente de red a otros Servidores de administración, puede utilizar las reglas de conmutación. Esta función solo es compatible con agentes de red instalados en dispositivos con Windows o macOS.

Las reglas de conmutación pueden activarse al cambiar los siguientes parámetros de red:

- Dirección de la puerta de enlace predeterminada.
- Dirección IP del servidor del DHCP.
- Sufijo DNS de la subred.
- Dirección IP del servidor DNS de la red.
- Accesibilidad del dominio de Windows. Este parámetro solo está disponible para dispositivos con Windows.
- Dirección de subred y máscara.
- Dirección IP del servidor WINS de la red. Este parámetro solo está disponible para dispositivos con Windows.
- El nombre de dominio DNS o NetBIOS del dispositivo cliente.
- Capacidad de acceder a una dirección con SSL.

Cuando se han creado reglas de conmutación para que el Agente de red cambie de Servidor de administración, el Agente de red responde de esta manera a los cambios en los parámetros de red:

- Si la configuración de la red cumple con una de las reglas creadas, el Agente de red se conecta con el Servidor de administración especificado en esta regla. Las aplicaciones instaladas en dispositivos cliente cambian a directivas fuera de la oficina siempre que este comportamiento esté habilitado por una regla.
- Si no se aplica ninguna de las reglas, el Agente de red revertirá a la configuración predeterminada de la conexión con el Servidor de administración especificado durante la instalación. Las aplicaciones instaladas en dispositivos cliente vuelven a las directivas activas.
- Si el Servidor de administración no es accesible, el Agente de red utilizará las directivas fuera de la oficina.

Para que el Agente de red pase a utilizar una directiva fuera de la oficina, es necesario que la opción **Habilitar el modo fuera de la oficina cuando el Servidor de administración no esté disponible** esté habilitada en la directiva del Agente de red.

La configuración de la conexión del Agente de red al Servidor de administración se guarda en un perfil de conexión. En el perfil de conexión puede crear reglas para cambiar dispositivos cliente a directivas fuera de la oficina además de configurar el perfil para que pueda utilizarse solo para descargar actualizaciones.

# Creación de una regla de conmutación del Agente de red por ubicación de red

Para que el Agente de red pueda cambiar de Servidor de administración según la ubicación de red del dispositivo, el dispositivo debe utilizar Windows o macOS.

*Para crear una regla para que el Agente de red cambie de un Servidor de administración a otro si la configuración de la red cambia:*

1. En el árbol de consola, seleccione el grupo de administración que contiene los dispositivos en los que necesita crear una regla de conmutación del Agente de red basada en la descripción de la ubicación de red.
2. Realice una de las siguientes acciones:
   - Si desea crear una regla para todos los dispositivos del grupo, vaya al espacio de trabajo del grupo y seleccione una directiva de Agente de red en la pestaña **Directivas**. Abra la ventana de propiedades de la directiva seleccionada.
   - Si tiene que crear una regla para un dispositivo seleccionado de un grupo, vaya al espacio de trabajo del grupo, seleccione el dispositivo en la pestaña **Dispositivos** y realice las siguientes acciones:
     a. Abra la ventana de propiedades del dispositivo seleccionado.
     b. En la sección **Aplicaciones** de la ventana de propiedades del dispositivo seleccione Agente de red.
     c. Abra la ventana de propiedades del Agente de red.
3. En la ventana de **Propiedades** que se abre, en la sección **Conectividad**, seleccione la subsección **Perfiles de conexión**.
4. En la sección **Configuración de ubicaciones de red**, haga clic en el botón **Agregar**.
5. En la ventana **Nueva descripción** que se abre, configure la descripción de la ubicación de red y la regla de conmutación. Especifique los siguientes parámetros de la descripción de la ubicación de red:
   - Nombre de la descripción de ubicación de red

     El nombre de una descripción de ubicación de red no puede ser más largo que 255 caracteres, ni contener símbolos especiales, por ejemplo ("*<>?\/:|).
   - Usar perfil de conexión

     En la lista desplegable, puede especificar el perfil de conexión que utiliza el Agente de red para conectarse al Servidor de administración. Este perfil se utilizará cuando las condiciones de la descripción de la ubicación de red se cumplan. El perfil de conexión contiene la configuración para conectar al Agente de red al Servidor de administración; también define cuándo los dispositivos cliente deben cambiar a las directivas fuera de la oficina. El perfil se utiliza solamente para descargar actualizaciones.

6. En la sección **Condiciones de cambio**, haga clic en el botón **Agregar** para crear una lista de condiciones para la descripción de la ubicación de red.

   Las condiciones de una regla se combinan con el operador lógico AND. Para desencadenar una regla que cambia por la descripción de la ubicación de la red, todas las reglas de conmutación de las condiciones se deben cumplir.

7. En la lista desplegable, seleccione el valor que corresponde al cambio en las características de la red a la que está conectado el dispositivo cliente:

   - **Dirección de la puerta de enlace de conexión predeterminada**: cambia la dirección de la puerta de enlace principal de la red.
   - **Dirección del servidor DHCP**: La dirección IP del servidor del Protocolo de configuración dinámica de host (DHCP) de la red ha cambiado.
   - **Dominio DNS**: cambió el sufijo DNS de la subred.
   - **Dirección del servidor DNS**: la dirección IP del servidor DNS de la red ha cambiado.
   - **Accesibilidad del dominio de Windows (solo para Windows)**: cambia el estado del dominio de Windows al cual está conectado el dispositivo cliente. Use este parámetro únicamente para dispositivos con Windows.
   - **Subred**: cambia la máscara y la dirección de subred.
   - **Dirección del servidor WINS (solo para Windows)**: cambió la dirección IP del servidor WINS de la red. Use este parámetro únicamente para dispositivos con Windows.
   - **Capacidad de resolver nombre**: el nombre DNS o NetBIOS del dispositivo cliente cambió.
   - **Acceso a dirección con SSL**: el dispositivo cliente puede o no puede (según la opción que seleccione) establecer una conexión SSL con un servidor específico (nombre:puerto). Para cada servidor, además puede especificar un certificado SSL. En este caso, el Agente de red verifica el certificado del servidor además de verificar la capacidad de una conexión SSL. Si el certificado no coincide, la conexión genera un error. La frecuencia de conexión es una vez por minuto.

8. En esta ventana que se abre, especifique la condición para que el Agente de red cambie a otro Servidor de administración. El nombre de la ventana depende del valor seleccionado en el paso anterior. Especifique la configuración siguiente de la condición de conmutación:

   - **Valor**

     En el campo, puede agregar uno o varios valores de la condición que se crea.

   - **Coincide al menos con un valor de la lista**

     Si se selecciona esta opción, la condición se cumplirá independientemente de los valores especificados en la lista **Valor**.

     Esta opción está seleccionada de forma predeterminada.

   - **No coincide con ningún valor de la lista**

     Si se selecciona esta opción, se cumple la condición si el valor de ésta no se encuentra en la lista **Valor**.

9. En la ventana **Nueva descripción**, seleccione la opción **Descripción habilitada** para habilitar el uso de la nueva descripción de ubicación de red.

Se creará una nueva regla de conmutación según la descripción de la ubicación de red; cada vez que las condiciones se cumplan, el Agente de red utilizará el perfil de conexión especificado en la regla para conectarse al Servidor de administración.

Las características de una red se comparan con las descripciones siguiendo el orden en el que estas últimas aparecen en la lista. Si una red coincide con varias descripciones, se utilizará la primera. Puede cambiar el orden de las reglas de la lista utilizando los botones **Arriba** (↑) y **Abajo** (↓).

## Notificación de eventos

Esta sección describe cómo seleccionar un método para entregar notificaciones del administrador sobre eventos en dispositivos cliente, y cómo ajustar la configuración de la notificación del evento.

También describe cómo probar la distribución de notificaciones de eventos usando el virus de prueba Eicar.

## Configuración de la notificación de eventos

Kaspersky Security Center le permite seleccionar un método para notificar al administrador sobre los eventos que ocurrieron en dispositivos cliente y configurar las notificaciones:

- Correo electrónico. Cuando ocurre un evento, la aplicación envía una notificación a las direcciones de correo electrónico especificadas. Puede editar el texto de la notificación.
- SMS. Cuando ocurre un evento, la aplicación envía una notificación a los números de teléfono especificados. Puede configurar las notificaciones por SMS para que se envíen a través de la pasarela de correo.
- Archivo ejecutable. Cuando ocurre un evento en un dispositivo, se inicia el archivo ejecutable en la estación de trabajo del administrador. Usando el archivo ejecutable, el administrador puede recibir los parámetros de cualquier evento que haya ocurrido.

*Para configurar notificaciones de eventos que ocurrieron en los dispositivos cliente:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la pestaña **Eventos**.
3. Haga clic en el enlace **Configurar notificaciones y la exportación de eventos** y seleccione el valor **Configurar notificaciones** en la lista desplegable.

   Esto abre la ventana **Propiedades: Eventos**.

4. En la sección **Notificación**, seleccione un método de notificación (por SMS, correo electrónico o al abrir un archivo ejecutable) y configure la notificación:

   - Correo electrónico

La pestaña **Correo electrónico** permite configurar las notificaciones de correo electrónico para eventos.

En el campo **Destinatarios (direcciones de correo electrónico)**, especifique las direcciones de correo electrónico a las que la aplicación enviará notificaciones. Puede especificar varias direcciones en este campo, separándolas con punto y coma.

En el campo **Servidores SMTP**, especifique las direcciones del servidor de correo, separándolas con punto y coma. Puede utilizar los siguientes parámetros:

- Dirección IPv4 o IPv6
- Nombre de la red de Windows (nombre NetBIOS) del dispositivo
- Nombre DNS del servidor SMTP

En el campo **Puerto de los servidores SMTP**, especifique el número de un puerto de comunicación del servidor SMTP. El número de puerto predeterminado es 25.

Si habilita la opción **Buscar registros MX por DNS**, puede utilizar varios registros MX de las direcciones IP para el mismo nombre DNS del servidor SMTP. El mismo nombre DNS puede tener varios registros MX con diferentes valores de prioridad de recepción de mensajes de correo electrónico. El Servidor de administración intenta enviar notificaciones del correo electrónico al servidor SMTP en orden ascendente de prioridad de registros MX. Esta opción está deshabilitada de forma predeterminada.

Si habilita la opción **Buscar registros MX por DNS** y no habilita el uso de la configuración de TLS, le recomendamos que use la configuración de DNSSEC en el dispositivo de su servidor como medida adicional de protección en el envío de notificaciones del correo electrónico.

Haga clic en el enlace **Configuración** para definir más ajustes de notificaciones:

- Nombre del sujeto (nombre del sujeto de un mensaje de correo electrónico)
- Dirección de correo electrónico del remitente
- Configuración de autenticación ESMTP

Debe especificar una cuenta para autenticar en un servidor SMTP si la opción de autenticación de ESMTP está habilitada para el servidor SMTP.

- Configuración de TLS para el servidor SMTP:
  - **No utilizar TLS**

    Puede seleccionar esta opción si desea deshabilitar el cifrado de mensajes de correo electrónico.
  - **Utilizar TLS si es compatible con el servidor SMTP**

    Puede seleccionar esta opción si desea usar una conexión TLS con un servidor SMTP. Si el servidor SMTP no es compatible con TLS, el Servidor de administración se conecta con el servidor SMTP sin usar TLS.
  - **Utilizar siempre TLS, comprobar la validez del certificado del servidor**

    Puede seleccionar esta opción si desea usar la configuración de autenticación de TLS. Si el servidor SMTP no es compatible con TLS, el Servidor de administración no puede conectarse al servidor SMTP.

Le recomendamos que use esta opción para una mejor protección de la conexión con un servidor SMTP. Si selecciona esta opción, puede establecer la configuración de autenticación para una conexión TLS.

Si elige el valor **Always use TLS, check the server certificate for validity**, puede especificar un certificado para la autenticación del servidor SMTP y elegir si desea habilitar la comunicación a través de cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. También puede especificar un certificado para la autenticación de un cliente en el servidor SMTP.

Puede especificar la configuración de TLS para un servidor SMTP:

- Busque un archivo de certificados del servidor SMTP:

Puede recibir un archivo con la lista de certificados de una autoridad de certificación confiable y cargar el archivo al Servidor de administración. Kaspersky Security Center verifica si el certificado de un servidor SMTP también está firmado por una autoridad de certificación confiable. Si el certificado de un servidor SMTP no se recibe de una autoridad de certificación confiable, Kaspersky Security Center no podrá conectarse al servidor SMTP.

- Busque un archivo de certificados cliente:

Puede utilizar un certificado recibido de cualquier fuente (por ejemplo, de una entidad de certificación de confianza). Deberá especificar el certificado y su clave privada. Puede usar, para ello, alguno de los siguientes tipos de certificado:

- Certificado X-509:

Debe especificar un archivo con el certificado y un archivo con la clave privada. Estos dos archivos no dependen el uno del otro y el orden en que se los carga no es importante. Cuando se cargan ambos archivos, debe especificar la contraseña para decodificar la clave privada. Si la clave privada no está codificada, puede dejar la contraseña en blanco.

- contenedor pkcs12:

Debe cargar un solo archivo que contenga el certificado y la clave privada. Cuando se carga el archivo, debe especificar la contraseña para decodificar la clave privada. Si la clave privada no está codificada, puede dejar la contraseña en blanco.

El campo **Mensaje de notificación** contiene texto estándar con información sobre el evento que la aplicación envía cuando ocurre un evento. Este texto incluye parámetros sustitutos, como el nombre del evento, el nombre del dispositivo y el nombre del dominio. Puede editar el texto del mensaje agregando otros parámetros sustitutos con detalles más relevantes del evento. La lista de parámetros sustitutos está disponible haciendo clic en el botón a la derecha del campo.

Si el texto de la notificación contiene un signo de porcentaje (%), debe escribirlo dos veces seguidas para permitir el envío de mensajes. Por ejemplo: "La carga de la CPU es 100 %%".

Haga clic en el vínculo **Configurar el límite numérico de notificaciones** para especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

Haga clic en el botón **Enviar mensaje de prueba** para verificar si configuró las notificaciones correctamente. La aplicación debería enviar una notificación de prueba a las direcciones de correo electrónico que especificó.

- SMS

La pestaña **SMS** permite configurar la transmisión de notificaciones por SMS de diversos eventos a un teléfono celular. Los mensajes SMS se envían a través de una pasarela de correo.

En el campo **Destinatarios (direcciones de correo electrónico)**, especifique las direcciones de correo electrónico a las que la aplicación enviará notificaciones. Puede especificar varias direcciones en este campo, separándolas con punto y coma. Las notificaciones se enviarán a los números de teléfono asociados con las direcciones de correo electrónico especificadas.

En el campo **Servidores SMTP**, especifique las direcciones del servidor de correo, separándolas con punto y coma. Puede utilizar los siguientes parámetros:

- Dirección IPv4 o IPv6
- Nombre de la red de Windows (nombre NetBIOS) del dispositivo
- Nombre DNS del servidor SMTP

En el campo **Puerto del servidor SMTP**, especifique el número de un puerto de comunicación del servidor SMTP. El número de puerto predeterminado es 25.

Haga clic en el enlace **Configuración** para definir más ajustes de notificaciones:

- Nombre del sujeto (nombre del sujeto de un mensaje de correo electrónico)
- Dirección de correo electrónico del remitente
- Configuración de autenticación ESMTP

En caso de ser necesario, puede especificar una cuenta para autenticar en un servidor SMTP si la opción de autenticación de ESMTP está habilitada para un servidor SMTP.

- Configuración de TLS para un servidor SMTP

Puede deshabilitar el uso de TLS, usar TLS si el servidor SMTP admite este protocolo o forzar el uso de TLS únicamente. Si elige usar solo TLS, puede especificar un certificado para la autenticación del servidor SMTP y elegir si desea habilitar la comunicación a través de cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. Además, si elige usar solo TLS, puede especificar un certificado para la autenticación del cliente en el servidor SMTP.

- Busque un archivo de certificados del servidor SMTP

Puede recibir un archivo con la lista de certificados de una autoridad de certificación confiable y cargar el archivo a Kaspersky Security Center. Kaspersky Security Center verifica si el certificado del servidor SMTP también está firmado por una autoridad de certificación confiable. Si el certificado del servidor SMTP no se recibe de una autoridad de certificación confiable, Kaspersky Security Center no podrá conectarse al servidor SMTP.

Debe cargar un solo archivo que contenga el certificado y la clave privada. Cuando se carga el archivo, debe especificar la contraseña para decodificar la clave privada. La contraseña puede estar vacía si la clave privada no se encripta. El campo **Mensaje de notificación** contiene texto estándar con información sobre el evento que la aplicación envía cuando ocurre un evento. Este texto incluye parámetros sustitutos, como el nombre del evento, el nombre del dispositivo y el nombre del dominio. Puede editar el texto del mensaje agregando otros parámetros sustitutos con detalles más relevantes del evento. La lista de parámetros sustitutos está disponible haciendo clic en el botón a la derecha del campo.

Si el texto de la notificación contiene un signo de porcentaje (%), debe escribirlo dos veces seguidas para permitir el envío de mensajes. Por ejemplo: "La carga de la CPU es 100 %%".

Haga clic en el vínculo **Configurar límite numérico de notificaciones** para especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

Haga clic en el botón **Enviar mensaje de texto** para verificar si configuró las notificaciones correctamente. La aplicación debería enviar una notificación de prueba al destinatario que especificó.

- Archivo para ejecutar

  Si se selecciona este método de notificación, en el campo de entrada puede especificar la aplicación que se iniciará cuando ocurra un evento.

  Al hacer clic en el enlace **Configurar el límite numérico de notificaciones** podrá especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

  Al hacer clic en el botón **Enviar mensaje de prueba**, podrá verificar si configuró las notificaciones correctamente: la aplicación envía una notificación de prueba a las direcciones de correo electrónico que especificó.

5. En el campo **Mensaje de notificación**, escriba el texto que la aplicación enviará cuando se produzca un evento.

   Puede usar la lista desplegable a la derecha del campo de texto para agregar una configuración de sustitución con detalles del evento (por ejemplo, descripción del evento u hora en la que ocurre).

   Si el texto de la notificación contiene un porcentaje (%), lo debe especificar dos veces seguidas para permitir el envío del mensaje. Por ejemplo: "La carga de la CPU es 100 %%".

6. Haga clic en el botón **Enviar mensaje de prueba** para comprobar si la notificación se configuró correctamente.

   La aplicación envía una notificación de prueba al usuario especificado.

7. Haga clic en **Aceptar** para guardar los cambios.

Se implementa la configuración de notificación modificada en todos los eventos que ocurrieron en dispositivos cliente.

Puede anular la configuración de notificación para ciertos eventos en la sección **Configuración de eventos** de la configuración del Servidor de administración, de una configuración de directiva o de una configuración de aplicación.

## Notificaciones de prueba

Para verificar si se envían las notificaciones de eventos, la aplicación usa la notificación de detección de "virus" de prueba EICAR en los dispositivos cliente.

*Para comprobar el envío de las notificaciones de eventos, haga lo siguiente:*

1. Detenga la tarea de protección del sistema de archivos en tiempo real en un dispositivo cliente y copie el "virus" de prueba EICAR en ese equipo cliente. Ahora vuelva a habilitar la protección en tiempo real del sistema de archivos.

2. Ejecute una tarea de análisis para los dispositivos cliente de un grupo de administración o para una serie de dispositivos específicos, incluido uno que tenga el "virus" EICAR.

   Si la tarea de análisis se configuró correctamente, se detectará el "virus" de prueba. Si las notificaciones se configuraron correctamente, recibirá una notificación informándole que se detectó un virus.

   En el espacio de trabajo del nodo del **Servidor de administración**, en la pestaña **Eventos**, la selección **Eventos recientes** muestra un registro de la detección de un "virus".

El "virus" de prueba EICAR no contiene código que pueda dañar su dispositivo. Sin embargo, las aplicaciones de seguridad de la mayoría de los fabricantes identifican este archivo como virus. Puede descargar el virus de prueba del sitio web oficial de EICAR.

## Notificaciones de eventos que se muestran al ejecutar un archivo ejecutable

Kaspersky Security Center puede notificar al administrador acerca de los eventos en dispositivos cliente al abrir un archivo ejecutable. El archivo ejecutable debe contener otro archivo ejecutable con marcadores del evento que se transmitirá al administrador (consulte la siguiente tabla).

Marcadores para describir un evento

| Marcador | Descripción del marcador |
|---|---|
| %SEVERITY% | Gravedad del evento. Valores posibles:<br>• **Información**<br>• **Advertencia**<br>• **Error**<br>• **Crítico** |
| %COMPUTER% | Nombre del dispositivo en el cual sucedió el evento.<br>La longitud máxima del nombre del dispositivo es de 256 caracteres. |
| %DOMAIN% | Nombre de dominio del dispositivo en el cual sucedió el evento. |
| %EVENT% | Nombre del tipo de evento.<br>La longitud máxima del nombre del tipo de evento es de 50 caracteres. |
| %DESCR% | Descripción del evento.<br>La longitud máxima de la descripción es de 1000 caracteres. |
| %RISE_TIME% | Hora de creación del evento. |
| %KLCSAK_EVENT_TASK_DISPLAY_NAME% | Nombre de la tarea.<br>La longitud máxima del nombre de la tarea es de 100 caracteres. |
| %KL_PRODUCT% | Nombre de la aplicación. |
| %KL_VERSION% | Número de versión de la aplicación. |
| %KLCSAK_EVENT_SEVERITY_NUM% | Número de gravedad del evento. Valores posibles:<br>• 1—**Información**<br>• 2—**Advertencia**<br>• 3—**Error**<br>• 4—**Crítico** |

| Marcador | Descripción del marcador |
| --- | --- |
| %HOST_IP% | Dirección IP del dispositivo en el cual sucedió el evento. |
| %HOST_CONN_IP% | Dirección IP de conexión del dispositivo en el cual sucedió el evento. |

Ejemplo:
Las notificaciones de eventos se envían a través de un archivo ejecutable (como script1.bat) dentro del que se inicia otro archivo ejecutable (como script2.bat) con el marcador %COMPUTER%. Cuando sucede un evento, el archivo script1.bat se ejecuta en el dispositivo del administrador, que a su vez ejecuta el archivo script2.bat con el marcador %COMPUTER%. El administrador luego recibe el nombre del dispositivo en el cual sucedió el evento.

# Cifrar la comunicación con TLS

Para corregir vulnerabilidades en la red corporativa de su organización, puede habilitar el cifrado de tráfico mediante el protocolo TLS. Puede habilitar los protocolos de cifrado TLS y los conjuntos de cifrado compatibles en el Servidor de administración y el Servidor MDM de iOS. Kaspersky Security Center admite las versiones 1.0, 1.1, 1.2 y 1.3 del protocolo TLS. Puede seleccionar el protocolo y los conjuntos de cifrado requeridos.

Kaspersky Security Center utiliza certificados autofirmados. No se requiere configuración adicional de los dispositivos iOS. También puede utilizar sus propios certificados. Los especialistas de Kaspersky recomiendan utilizar certificados emitidos por autoridades de certificación de confianza.

## Servidor de administración

*Para configurar los protocolos de cifrado permitidos y las suites de cifrado en el Servidor de administración:*

1. Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada es <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Utilice el indicador SrvUseStrictSslSettings para configurar los protocolos y los conjuntos de cifrado permitidos en el Servidor de administración. Ingrese el siguiente comando:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <valor> -t d
   ```

   Especifique el parámetro <valor> del indicador SrvUseStrictSslSettings flag:

   - 4—Solo están habilitados los protocolos TLS 1.2 y TLS 1.3. También están habilitados los conjuntos de cifrado con TLS_RSA_WITH_AES_256_GCM_SHA384 (estos conjuntos de cifrado son necesarios para la compatibilidad con versiones anteriores de Kaspersky Security Center). Este es el valor predeterminado.

     Conjuntos de cifrado compatibles con el protocolo TLS 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384 (conjunto de cifrado con TLS_RSA_WITH_AES_256_GCM_SHA384)
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     Conjuntos de cifrado compatibles con el protocolo TLS 1.3:

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256
     - TLS_AES_128_GCM_SHA256
     - TLS_AES_128_CCM_SHA256

   - 5—Solo están habilitados los protocolos TLS 1.2 y TLS 1.3. Para el protocolo TLS 1.2 y TLS 1.3, se admiten los conjuntos de cifrado específicos que se enumeran a continuación.

     Conjuntos de cifrado compatibles con el protocolo TLS 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - ECDHE-RSA-AES128-GCM-SHA256

- ECDHE-RSA-AES128-SHA256

Conjuntos de cifrado compatibles con el protocolo TLS 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

No recomendamos usar 0, 1, 2 o 3 como valor de parámetro del indicador SrvUseStrictSslSettings. Estos valores de parámetros corresponden a versiones del protocolo TLS no seguras (los protocolos TLS 1.0 y TLS 1.1) y conjuntos de cifrado no seguros, y se utilizan solo para la compatibilidad con versiones anteriores de Kaspersky Security Center.

3. Reinicie los siguientes servicios de Kaspersky Security Center 15.1:

- Servidor de administración
- Servidor web
- Proxy de activación

Se habilita el cifrado de tráfico mediante el protocolo TLS.

Puede utilizar los indicadores KLTR_TLS12_ENABLED y KLTR_TLS13_ENABLED para habilitar la compatibilidad con los protocolos TLS 1.2 y TLS 1.3, respectivamente. Estos indicadores están habilitados de manera predeterminada.

*Para habilitar o deshabilitar la compatibilidad con los protocolos TLS 1.2 y TLS 1.3:*

1. Ejecute la utilidad klscflag.

   Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada es <Disk>:\Archivos de programa(x86)\Kaspersky Lab\Kaspersky Security Center.

2. Ingrese uno de los siguientes comandos en el símbolo del sistema de Windows, usando derechos de administrador:

   - Utilice este comando para habilitar o deshabilitar la compatibilidad con el protocolo TLS 1.2:

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <valor> -t d
     ```

   - Utilice este comando para habilitar o deshabilitar la compatibilidad con el protocolo TLS 1.3:

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <valor> -t d
     ```

   Especifique el parámetro `<valor>` del indicador:

   - `1`—Para habilitar el soporte del protocolo TLS.
   - `0`—Para deshabilitar el soporte del protocolo TLS.

### Servidor de MDM para iOS

La conexión entre los dispositivos iOS y el Servidor de MDM para iOS está cifrada de forma predeterminada.

*Para configurar los protocolos de cifrado permitidos y las suites de cifrado en el servidor de MDM para iOS:*

1. Abra el registro del sistema del dispositivo cliente en el que está instalado el Servidor de MDM para iOS (por ejemplo, de forma local con el comando regedit en el menú **Iniciar** → **Ejecutar**).
2. Vaya al siguiente archivo:
   - Para sistemas de 32 bits:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Cor
   - Para sistemas de 64 bits:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSI
3. Cree una clave de nombre `StrictSslSettings`.
4. Especifique `DWORD` como tipo de clave.
5. Configure el valor de clave:
   - `2`: Están habilitados los protocolos TLS 1.0, TLS 1.1 y TLS 1.2.
   - `3`: Solo está habilitado el protocolo TLS 1.2 (valor predeterminado).
6. Reinicie el servicio del Servidor de MDM para iOS de Kaspersky Security Center.

# Configuración de la interfaz

Puede configurar la interfaz de Kaspersky Security Center de distintas maneras:

- Puede definir qué objetos se mostrarán o no en el árbol de la consola, en el espacio de trabajo y en las ventanas de propiedades de los objetos (carpetas, secciones) en función de las características que utilice.
- Puede definir cuáles elementos de la ventana principal se mostrarán o no (por ejemplo, el árbol de la consola o los menús estándar como **Acciones** y **Ver**).

*Para configurar la interfaz de Kaspersky Security Center y adaptarla a las características que utilice:*

1. En el árbol de consola, haga clic el nodo del **Servidor de administración**.
2. En la ventana principal de la aplicación, diríjase a la barra de menús y seleccione **Ver** → **Configuración de interfaz**.

3. En la ventana **Configuración de interfaz** que se abre, utilice las siguientes casillas para definir si los elementos correspondientes se mostrarán o no:

- Mostrar Administración de vulnerabilidades y parches

  Si se habilita esta opción, la carpeta **Instalación remota** incluirá una subcarpeta llamada **Desplegar imágenes de dispositivos**, y la carpeta **Repositorios** incluirá una subcarpeta llamada **Hardware**.

  De manera predeterminada, esta opción se deshabilita si el Asistente de inicio rápido no ha finalizado. De manera predeterminada, esta opción se habilita una vez que el Asistente de inicio rápido ha finalizado.

  Si esta opción no está habilitada, los elementos del menú **Crear sesiones de RDP** y **Windows Desktop Sharing** no estarán disponibles aunque exista una licencia para Administración de sistemas.

- Mostrar Protección y cifrado de datos

  Si se habilita esta opción, el árbol de la consola muestra la carpeta **Protección y cifrado de datos**.

  Esta opción está activada de forma predeterminada.

- Mostrar Configuración de Control de Endpoint

  Si se habilita esta opción, las siguientes subsecciones se muestran en la sección **Controles de seguridad** de la ventana de propiedades de la directiva de Kaspersky Endpoint Security para Windows:

  - **Control de aplicaciones**
  - **Control de dispositivos**
  - **Control web**
  - **Control de anomalías adaptativo**

  Si se deshabilita esta opción, estas subsecciones no se mostrarán en la sección **Controles de seguridad**.

  Esta opción está activada de forma predeterminada.

- Mostrar Administración de dispositivos móviles

  Si se habilita esta opción, la característica **Administración de dispositivos móviles** estará disponible. Una vez que reinicie la aplicación, encontrará una carpeta llamada **Dispositivos móviles** en el árbol de la consola.

  Esta opción está activada de forma predeterminada.

- Mostrar Servidores de administración secundarios

Si activa esta casilla, los nodos de los Servidores de administración secundarios y virtuales se mostrarán dentro de los grupos de administración en el árbol de la consola. Esto le permitirá utilizar las funcionalidades diseñadas para trabajar con Servidores de administración secundarios y virtuales; por ejemplo, podrá crear tareas de instalación remota en Servidores de administración secundarios.

Esta casilla no está marcada de manera predeterminada.

- Mostrar secciones de configuración de seguridad

  Si se habilita esta opción, encontrará una sección llamada **Seguridad** en la ventana de propiedades del Servidor de administración, de los grupos de administración y de otros objetos. Esta opción le permitirá asignar a los usuarios y a los grupos de usuarios permisos personalizados para trabajar con objetos.

  Esta opción está deshabilitada de forma predeterminada.

4. Haga clic en **Aceptar**.

Para aplicar ciertos cambios, deberá cerrar y volver a abrir la ventana principal de la aplicación.

*Para definir qué elementos se mostrarán en la ventana principal de la aplicación:*

1. En la ventana principal de la aplicación, diríjase a la barra de menús y seleccione **Ver** → **Configurar**.
2. En la ventana **Configuración de vista** que se abre, utilice las casillas para definir qué elementos se mostrarán en la ventana principal de la aplicación.
3. Haga clic en **Aceptar**.

# Descubrimiento de dispositivos conectados a la red

Esta sección describe los pasos que debe seguir después de la instalación de Kaspersky Security Center.

## Escenario: Descubrir dispositivos conectados a la red

Antes de instalar las aplicaciones de seguridad, es necesario llevar a cabo un descubrimiento de dispositivos. El Servidor de administración recibe información sobre los dispositivos descubiertos y le permite administrar los dispositivos a través de directivas. Se necesitan sondeos de red regulares para actualizar la lista de dispositivos disponibles en la red.

Antes de iniciar el sondeo de red, asegúrese de que el protocolo SMB esté habilitado. De lo contrario, Kaspersky Security Center no puede detectar dispositivos en la red sondeada. Para habilitar el protocolo SMB, siga las instrucciones para su sistema operativo.

La detección de dispositivos en red se realiza en las siguientes etapas:

1. **Descubrir dispositivos**

Utilice el Asistente de inicio rápido para realizar un descubrimiento de dispositivos inicial y detectar computadoras, tablets, teléfonos móviles y otros dispositivos conectados a la red. También puede realizar el descubrimiento de dispositivos manualmente.

2. **Configurar sondeos programados**

   Decida qué tipo(s) de sondeo desea utilizar regularmente. Habilite los tipos deseados y configure la programación del sondeo. Puede referirse a las recomendaciones para la frecuencia de sondeo de red.

3. **Configurar reglas para que los dispositivos descubiertos se agreguen a grupos de administración (opcional)**

   Si aparecen nuevos dispositivos de la red, que se detectan durante las encuestas regulares y se incluyen automáticamente en el grupo **Dispositivos no asignados**. Puede configurar reglas de movimiento de dispositivos para automatizar la asignación de dispositivos al grupo **Dispositivos administrados**. También puede configurar las reglas de retención.

   Si omite el paso 3, los dispositivos recién descubiertos se asignan al grupo **Dispositivos no asignados**. Si lo desea, puede mover estos dispositivos manualmente al grupo **Dispositivos administrados**. Si mueve los dispositivos manualmente al grupo **Dispositivos administrados**, puede analizar la información sobre cada dispositivo y decidir si desea moverlo a un grupo de administración, y, de ser así, a qué grupo exacto.

### Resultados

Completar las etapas anteriores tiene los siguientes resultados:

- El Servidor de administración de Kaspersky Security Center detecta los dispositivos que están en la red y le proporciona información sobre ellos.
- Los sondeos futuros se configuran y funcionan de acuerdo con el calendario programado.
- Los dispositivos recién descubiertos se arreglan según las reglas configuradas. (O, si no se configura ninguna regla, los dispositivos se quedan en el grupo **Dispositivos no asignados**).

# Dispositivos no asignados

Esta sección proporciona información sobre cómo administrar los dispositivos de una red empresarial si no están incluidos en un grupo de administración.

## Descubrimiento de dispositivos

Esta sección describe los tipos de descubrimiento de dispositivos disponibles en Kaspersky Security Center y proporciona información sobre cada tipo.

El Servidor de administración recibe información sobre la estructura de la red y los dispositivos en esta red a través de un sondeo regular. La información se registra en la base de datos del Servidor de administración. El Servidor de administración puede utilizar los siguientes tipos de sondeo:

- **Sondeo de la red de Windows**. El Servidor de administración puede realizar dos tipos de sondeos de red de Windows: rápida y completa. Cuando se realiza un sondeo rápido, el Servidor de administración solo recupera información de la lista de nombres NetBIOS correspondientes a los dispositivos de todos los dominios y grupos de trabajo de la red. Durante un sondeo completo, se solicita más información desde cada dispositivo cliente, como el nombre del sistema operativo, la dirección IP, el nombre DNS y el nombre NetBIOS. De forma predeterminada, tanto el sondeo rápido como el sondeo completo están habilitados. El sondeo de la red de Windows puede no detectar dispositivos, por ejemplo, si los puertos UDP 137, UDP 138, TCP 139 están cerrados en el enrutador o por el firewall.

- **Sondeo de Active Directory**. El Servidor de administración recupera información sobre la estructura de la unidad de Active Directory y sobre los nombres DNS de los dispositivos de los grupos de Active Directory. Por defecto, este tipo de sondeo está habilitado. Le recomendamos que utilice el sondeo de Active Directory si utiliza Active Directory; de lo contrario, el Servidor de administración no detecta ningún dispositivo. Si usa Active Directory, pero algunos de los dispositivos en red no figuran como miembros, estos dispositivos no pueden ser detectados por el sondeo de Active Directory.

- **Sondeo de intervalos IP**. El Servidor de administración utiliza paquetes ICMP o el protocolo NBNS para sondear los intervalos IP especificados y recopilar una serie de datos completa sobre los dispositivos incluidos en esos intervalos. Este tipo de sondeo está deshabilitado de manera predeterminada. No se recomienda usar este tipo de sondeo si ya realiza sondeos de la red de Windows o de Active Directory.

- **Sondeo de Zeroconf**. Un punto de distribución que sondea la red IPv6 mediante el uso de una red de configuración cero (también denominada *Zeroconf*). Este tipo de sondeo está deshabilitado de manera predeterminada. Puede usar el sondeo de Zeroconf si el punto de distribución ejecuta Linux.

Si configura y habilita reglas de movimiento de dispositivos, los dispositivos recién descubiertos se incluirán de forma automática en el grupo **Dispositivos administrados**. Si no se han habilitado reglas de movimiento, los dispositivos recién descubiertos se incluyen automáticamente en el grupo **Dispositivos no asignados**.

Puede modificar la configuración de descubrimiento de dispositivos para cada tipo. Por ejemplo, puede cambiar la frecuencia con la que se realizan los sondeos o definir si el sondeo del dominio alcanzará a todo el bosque o estará limitado a un dominio específico.

Antes de iniciar el sondeo de red, asegúrese de que el protocolo SMB esté habilitado. De lo contrario, Kaspersky Security Center no puede detectar dispositivos en la red sondeada. Para habilitar el protocolo SMB, siga las instrucciones para su sistema operativo.

## Sondeo de la red de Windows

### Acerca del sondeo de la red de Windows

Cuando se realiza un sondeo rápido, el Servidor de administración solo recupera información de la lista de nombres NetBIOS correspondientes a los dispositivos de todos los dominios y grupos de trabajo de la red. Cuando se realiza un sondeo completo, se solicita la siguiente información a cada dispositivo cliente:

- Nombre del sistema operativo

- Dirección IP

- Nombre DNS
- Nombre NetBIOS

Para realizar un sondeo rápido o completo, se deben cumplir los siguientes requisitos:

- Los puertos UDP 137/138, TCP 139, UDP 445, TCP 445 deben estar disponibles en la red.
- El protocolo SMB está activado.
- Se debe utilizar el servicio Explorador de equipos de Microsoft y el equipo del navegador principal debe estar habilitado en el Servidor de administración.
- Se debe utilizar el servicio Explorador de equipos de Microsoft y el equipo explorador principal debe estar habilitado en esta cantidad de dispositivos cliente:
  - al menos un dispositivo si no hay más de 32 dispositivos conectados a la red;
  - al menos un dispositivo por cada 32 dispositivos conectados a la red.

Para realizar un sondeo completo, primero debe haberse realizado al menos un sondeo rápido.

## Cómo ver y modificar la configuración del sondeo de la red de Windows

*Para modificar la configuración para el sondeo de la red de Windows:*

1. En el árbol de la consola, en la carpeta **Descubrimiento de dispositivos**, seleccione la subcarpeta **Dominios**.

   Puede pasar de la carpeta **Dispositivos no asignados** a la carpeta **Descubrimiento de dispositivos** haciendo clic en el botón **Sondear ahora**.

   En el espacio de trabajo de la subcarpeta **Dominios**, se muestra la lista de dispositivos.

2. Haga clic en **Sondear ahora**.

   Se abre la ventana de propiedades del dominio. Si lo desea, modifique la configuración del sondeo de la red de Windows:

   - Habilitar el sondeo de la red de Windows

     Esta opción está seleccionada de forma predeterminada. Si no desea realizar un sondeo de la red de Windows (por ejemplo, si cree que el sondeo de Active Directory es suficiente), puede retirar la selección de esta opción.

   - Establecer programación de sondeo rápido

De manera predeterminada, el período es de 15 minutos.

Cuando se realiza un sondeo rápido, el Servidor de administración solo recupera información de la lista de nombres NetBIOS correspondientes a los dispositivos de todos los dominios y grupos de trabajo de la red.

Los datos recibidos en un sondeo reemplazan completamente los datos del sondeo anterior.

Las siguientes opciones de horarios de sondeo están disponibles:

- **Cada N días**

  Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la fecha y hora indicadas. Cada sondeo estará separado del anterior por el número de días que indique.

  De forma predeterminada, se realizará un sondeo todos los días, a partir de la fecha y hora actuales del sistema.

- **Cada N minutos**

  Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la hora indicada. Cada sondeo estará separado del anterior por el número de minutos que indique.

  De forma predeterminada, se realizará un sondeo cada cinco minutos, a partir de la hora actual del sistema.

- **Por días de la semana**

  Se realizará un sondeo en forma periódica, a intervalos regulares, en el día de la semana y a la hora que indique.

  De manera predeterminada, el sondeo se ejecutará todos los viernes a las 18:00:00.

- **Cada mes en los días especificados de semanas seleccionadas**

  Se realizará un sondeo en forma periódica, a intervalos regulares, en los días del mes y a la hora que indique.

  Por defecto, no hay ningún día seleccionado; la hora de inicio predeterminada es las 18:00:00.

- **Ejecutar tareas no realizadas**

  Si el Servidor de administración está apagado o no está disponible durante la hora programada para el sondeo, el Servidor de administración puede iniciar el sondeo inmediatamente después de encenderlo o esperar la próxima vez que se programe el sondeo.

  Si esta opción está habilitada, el Servidor de administración inicia el sondeo inmediatamente después de que se enciende.

  Si esta opción está desactivada, el Servidor de administración espera la próxima vez que se programe el sondeo.

  Esta opción está activada de forma predeterminada.

- **Establecer programación de sondeo completo**

La frecuencia de sondeo predeterminada es de una hora. Los datos recibidos en un sondeo reemplazan completamente los datos del sondeo anterior.

Las siguientes opciones de horarios de sondeo están disponibles:

- **Cada N días**

  Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la fecha y hora indicadas. Cada sondeo estará separado del anterior por el número de días que indique.

  De forma predeterminada, se realizará un sondeo todos los días, a partir de la fecha y hora actuales del sistema.

- **Cada N minutos**

  Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la hora indicada. Cada sondeo estará separado del anterior por el número de minutos que indique.

  De forma predeterminada, se realizará un sondeo cada cinco minutos, a partir de la hora actual del sistema.

- **Por días de la semana**

  Se realizará un sondeo en forma periódica, a intervalos regulares, en el día de la semana y a la hora que indique.

  De manera predeterminada, el sondeo se ejecutará todos los viernes a las 18:00:00.

- **Cada mes en los días especificados de semanas seleccionadas**

  Se realizará un sondeo en forma periódica, a intervalos regulares, en los días del mes y a la hora que indique.

  Por defecto, no hay ningún día seleccionado; la hora de inicio predeterminada es las 18:00:00.

- **Ejecutar tareas no realizadas**

  Si el Servidor de administración está apagado o no está disponible durante la hora programada para el sondeo, el Servidor de administración puede iniciar el sondeo inmediatamente después de encenderlo o esperar la próxima vez que se programe el sondeo.

  Si esta opción está habilitada, el Servidor de administración inicia el sondeo inmediatamente después de que se enciende.

  Si esta opción está desactivada, el Servidor de administración espera la próxima vez que se programe el sondeo.

  Esta opción está activada de forma predeterminada.

Si desea realizar el sondeo inmediatamente, haga clic en **Sondear ahora**. Ambos tipos de sondeos comenzarán.

En el Servidor de administración virtual, puede ver y editar la configuración de sondeo de la red de Windows en la ventana de propiedades del punto de distribución, en la sección **Descubrimiento de dispositivos**.

## Sondeo de Active Directory

Utilice la función de sondeo de Active Directory si usa Active Directory; de lo contrario, recomendamos que opte por otra clase de sondeo. Si usa Active Directory, pero algunos de los dispositivos en red no figuran como miembros, estos dispositivos no pueden ser detectados por el sondeo de Active Directory.

Los resultados del sondeo de Active Directory se almacenan en el Servidor de administración durante 30 días, independientemente de los resultados del sondeo posterior.

Antes de iniciar el sondeo de red, asegúrese de que el protocolo SMB esté habilitado. De lo contrario, Kaspersky Security Center no puede detectar dispositivos en la red sondeada. Para habilitar el protocolo SMB, siga las instrucciones para su sistema operativo.

## Cómo ver y modificar la configuración del sondeo de Active Directory

*Para ver y modificar la configuración para el sondeo de grupos de Active Directory:*

1. En el árbol de la consola, en la carpeta **Descubrimiento de dispositivos**, seleccione la subcarpeta **Active Directory**.

   También puede pasar de la carpeta **Dispositivos no asignados** a la carpeta **Descubrimiento de dispositivos** haciendo clic en el botón **Sondear ahora**.

2. Haga clic en **Configurar sondeo**.

   Se abre la ventana Propiedades de Active Directory. Si lo desea, modifique la configuración de sondeo de grupo de Active Directory:

   - Habilitar el sondeo de Active Directory

     Esta opción está seleccionada de forma predeterminada. Sin embargo, si no usa Active Directory, el sondeo no recupera ningún resultado. En este caso, puede retirar la selección de esta opción.

   - Configurar programación de sondeos

La frecuencia de sondeo predeterminada es de una hora.

Las siguientes opciones de horarios de sondeo están disponibles:

- **Cada N días**

  Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la fecha y hora indicadas. Cada sondeo estará separado del anterior por el número de días que indique.

  De forma predeterminada, se realizará un sondeo todos los días, a partir de la fecha y hora actuales del sistema.

- **Cada N minutos**

  Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la hora indicada. Cada sondeo estará separado del anterior por el número de minutos que indique.

  De forma predeterminada, se realizará un sondeo cada cinco minutos, a partir de la hora actual del sistema.

- **Por días de la semana**

  Se realizará un sondeo en forma periódica, a intervalos regulares, en el día de la semana y a la hora que indique.

  De manera predeterminada, el sondeo se ejecutará todos los viernes a las 18:00:00.

- **Cada mes en los días especificados de semanas seleccionadas**

  Se realizará un sondeo en forma periódica, a intervalos regulares, en los días del mes y a la hora que indique.

  Por defecto, no hay ningún día seleccionado; la hora de inicio predeterminada es las 18:00:00.

- **Ejecutar tareas no realizadas**

  Si el Servidor de administración está apagado o no está disponible durante la hora programada para el sondeo, el Servidor de administración puede iniciar el sondeo inmediatamente después de encenderlo o esperar la próxima vez que se programe el sondeo.

  Si esta opción está habilitada, el Servidor de administración inicia el sondeo inmediatamente después de que se enciende.

  Si esta opción está desactivada, el Servidor de administración espera la próxima vez que se programe el sondeo.

  Esta opción está activada de forma predeterminada.

- **Avanzado**

Puede seleccionar qué dominios de Active Directory sondear:

- Dominio de Active Directory al que pertenece Kaspersky Security Center
- Bosque de dominio al que pertenece Kaspersky Security Center
- Lista especificada de dominios de Active Directory.

  Si selecciona esta opción, puede agregar dominios al ámbito de sondeo:

  - Haga clic en el botón **Agregar**.
  - En los campos correspondientes, especifique la dirección del controlador de dominio, y el nombre y la contraseña de la cuenta para acceder a él.
  - Haga clic en **Aceptar** para guardar los cambios.

  Puede seleccionar la dirección del controlador de dominio en la lista y hacer clic en los botones **Modificar** o **Eliminar** para modificarlo o eliminarlo.
- Haga clic en **Aceptar** para guardar los cambios.

Si desea realizar el sondeo inmediatamente, haga clic en el botón **Sondear ahora**.

En el Servidor de administración virtual, puede ver y editar la configuración de sondeo de los grupos de Active Directory en la ventana de propiedades del punto de distribución, en la sección **Descubrimiento de dispositivos**.

## Sondeo de intervalos IP

El Servidor de administración utiliza paquetes ICMP o el protocolo NBNS para sondear los intervalos IP especificados y recopilar una serie de datos completa sobre los dispositivos incluidos en esos intervalos. Este tipo de sondeo está deshabilitado de manera predeterminada.

Para todos los hosts basados en Linux dentro de un controlador de dominio de Microsoft Active Directory o Samba, especifique el `netbios name` y los parámetros del `workgroup` en el archivo `/etc/samba/smb.conf`. Si no lo hace, es posible que los resultados del sondeo contengan hosts duplicados.

Antes de iniciar el sondeo de red, asegúrese de que el protocolo SMB esté habilitado. De lo contrario, Kaspersky Security Center no puede detectar dispositivos en la red sondeada. Para habilitar el protocolo SMB, siga las instrucciones para su sistema operativo.

## Cómo ver y modificar la configuración del sondeo de intervalos IP

*Para ver y modificar la configuración de sondeo de los grupos de rango de IP:*

1. En el árbol de la consola, en la carpeta **Descubrimiento de dispositivos**, seleccione la subcarpeta **Intervalos IP**.

   Puede pasar de la carpeta **Dispositivos no asignados** a la carpeta **Descubrimiento de dispositivos** al hacer clic en la carpeta **Sondear ahora**.

2. Si lo desea, en la subcarpeta **Intervalos IP**, haga clic en **Agregar subred** para agregar un rango de IP para sondeo, y luego haga clic en **Aceptar**.

3. Haga clic en **Configurar sondeo**.

   Se abre la ventana de propiedades de Rangos IP. Si lo desea, puede modificar la configuración del sondeo de rango de IP:

   - **Habilitar el sondeo del intervalo IP**

     Esta opción no está seleccionada de manera predeterminada. No se recomienda usar este tipo de sondeo si ya realiza sondeos de la red de Windows o de Active Directory.

   - **Configurar programación de sondeos**

De manera predeterminada, el período es de 420 minutos. Los datos recibidos en un sondeo reemplazan completamente los datos del sondeo anterior.

Las siguientes opciones de horarios de sondeo están disponibles:

- **Cada N días**

  Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la fecha y hora indicadas. Cada sondeo estará separado del anterior por el número de días que indique.

  De forma predeterminada, se realizará un sondeo todos los días, a partir de la fecha y hora actuales del sistema.

- **Cada N minutos**

  Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la hora indicada. Cada sondeo estará separado del anterior por el número de minutos que indique.

  De forma predeterminada, se realizará un sondeo cada cinco minutos, a partir de la hora actual del sistema.

- **Por días de la semana**

  Se realizará un sondeo en forma periódica, a intervalos regulares, en el día de la semana y a la hora que indique.

  De manera predeterminada, el sondeo se ejecutará todos los viernes a las 18:00:00.

- **Cada mes en los días especificados de semanas seleccionadas**

  Se realizará un sondeo en forma periódica, a intervalos regulares, en los días del mes y a la hora que indique.

  Por defecto, no hay ningún día seleccionado; la hora de inicio predeterminada es las 18:00:00.

- **Ejecutar tareas no realizadas**

  Si el Servidor de administración está apagado o no está disponible durante la hora programada para el sondeo, el Servidor de administración puede iniciar el sondeo inmediatamente después de encenderlo o esperar la próxima vez que se programe el sondeo.

  Si esta opción está habilitada, el Servidor de administración inicia el sondeo inmediatamente después de que se enciende.

  Si esta opción está desactivada, el Servidor de administración espera la próxima vez que se programe el sondeo.

  Esta opción está activada de forma predeterminada.

Si desea realizar el sondeo inmediatamente, haga clic en **Sondear ahora**. Este botón solo está disponible si seleccionó **Habilitar el sondeo del intervalo IP**.

En el Servidor de administración virtual, puede ver y editar la configuración del sondeo de rango de IP en la ventana de propiedades del punto de distribución, en la sección **Descubrimiento de dispositivos**. Los dispositivos cliente detectados durante el sondeo de rangos IP se muestran en la carpeta **Dominios** del Servidor de administración virtual.

### Sondeo con Zeroconf

Este tipo de sondeo solo es compatible con los puntos de distribución basados en Linux.

Un punto de distribución puede sondear las redes que tienen dispositivos con direcciones IPv6. En este caso, no se especifican los rangos de IP y el punto de distribución sondea toda la red mediante el uso de una red de configuración cero (denominada *Zeroconf*). Para empezar a usar Zeroconf, debe instalar la utilidad avahi-browse en el punto de distribución.

*Para habilitar el sondeo de Zeroconf:*

1. En el árbol de la consola, en la carpeta **Descubrimiento de dispositivos**, seleccione la subcarpeta **Intervalos IP**.

   Puede pasar de la carpeta **Dispositivos no asignados** a la carpeta **Descubrimiento de dispositivos** al hacer clic en la carpeta **Sondear ahora**.

2. Haga clic en **Configurar sondeo**.

3. En la ventana de las propiedades de los rangos de IP que se abre, seleccione **Habilitar el sondeo con la tecnología Zeroconf**.

Después de esto, el punto de distribución empieza a sondear su red. En este caso, se ignoran los rangos de IP especificados.

## Trabajar con dominios de Windows. Ver y cambiar la configuración de dominio

*Para modificar la configuración de dominio:*

1. En el árbol de la consola, en la carpeta **Descubrimiento de dispositivos**, seleccione la subcarpeta **Dominios**.

2. Seleccione un dominio y abra su ventana de propiedades de una de las siguientes formas:

   - Seleccione **Propiedades** en el menú contextual del dominio.

   - Haga clic en el enlace **Mostrar propiedades de grupo**.

   La ventana **Propiedades: <Nombre del dominio>** se abre, desde la cual puede configurar el dominio seleccionado.

# Configuración de reglas de retención para dispositivos no asignados

Una vez finalizado el sondeo de la red de Windows, los dispositivos descubiertos se colocan en subgrupos del grupo de administración "Dispositivos no asignados". Este grupo de administración se puede encontrar en **Avanzado → Descubrimiento de dispositivos → Dominios**. El grupo principal es **Dominios**. Contiene grupos secundarios nombrados después de los dominios correspondientes y grupos de trabajo que se han encontrado durante el sondeo de red. El grupo primario también puede contener el grupo de administración de dispositivos móviles. Puede configurar las reglas de retención de dispositivos no asignados para el grupo primario y para cada uno de los grupos secundarios. Las reglas de retención no dependen de la configuración de sondeo de la red y funcionan incluso si el sondeo de la red está desactivado.

*Para configurar las reglas de retención para dispositivos no asignados:*

1. En el árbol de la consola, en la carpeta de **Descubrimiento de dispositivos**, realice una de las siguientes acciones:

   - Para configurar los ajustes del grupo principal, haga clic con el botón derecho en la subcarpeta **Dominios** y seleccione **Propiedades**.

     Se abrirá la ventana de propiedades del grupo principal.

   - Para configurar los ajustes de un grupo secundario, haga clic con el botón derecho en su nombre y seleccione **Propiedades**.

     Se abrirá la ventana de propiedades del grupo secundario.

2. En la sección **Dispositivos**, especifique la siguiente configuración:

   - **Eliminar el dispositivo del grupo si ha estado inactivo por más de (días)**

     Si esta opción está habilitada, puede especificar el intervalo de tiempo que se deja pasar antes de que el dispositivo se elimine del grupo automáticamente. De forma predeterminada, esta opción se propaga a los grupos secundarios. El intervalo de tiempo por defecto es de 7 días.

     Esta opción está activada de forma predeterminada.

   - **Heredar del grupo primario**

     Si esta opción está habilitada, el período de retención de dispositivos en el grupo seleccionado se heredará del grupo primario y no se podrá modificar.

     Esta opción solo está disponible para grupos secundarios.

     Esta opción está activada de forma predeterminada.

   - **Forzar herencia en grupos secundarios**

     Los valores de configuración se propagarán a los grupos secundarios. Los ajustes correspondientes estarán bloqueados en las propiedades de esos grupos.

     Esta opción está deshabilitada de forma predeterminada.

Se guardarán y aplicarán los cambios.

# Trabajar con rangos IP

Puede personalizar rangos IP existentes y crear nuevos.

## Crear un rango IP

*Para crear un rango IP:*

1. En el árbol de la consola, en la carpeta **Descubrimiento de dispositivos**, seleccione la subcarpeta **Intervalos IP**.
2. En el menú contextual de la carpeta, seleccione **Nuevo** → **Intervalo IP**.
3. En la ventana **Nuevo intervalo IP** que se abre, configure el nuevo rango IP.

El nuevo rango IP aparece en la carpeta **Intervalos IP**.

## Ver y modificar la configuración del rango IP

*Para modificar la configuración del rango IP:*

1. En el árbol de la consola, en la carpeta **Descubrimiento de dispositivos**, seleccione la subcarpeta **Intervalos IP**.
2. Seleccione un rango IP y abra su ventana de propiedades de una de las siguientes formas:
   - Seleccione **Propiedades** en el menú contextual del rango IP.
   - Haga clic en el enlace **Mostrar propiedades de grupo**.

La ventana **Propiedades: <Nombre del rango IP>** se abre, desde la cual puede configurar las propiedades del rango IP seleccionado.

# Trabajar con los grupos de Active Directory. Ver y cambiar la configuración de grupo

*Para modificar la configuración del grupo de Active Directory:*

1. En el árbol de la consola, en la carpeta **Descubrimiento de dispositivos**, seleccione la subcarpeta **Active Directory**.
2. Seleccione un grupo de Active Directory y abra su ventana de propiedades de una de las siguientes formas:
   - Seleccione **Propiedades** en el menú contextual del rango IP.
   - Haga clic en el enlace **Mostrar propiedades de grupo**.

La ventana **Propiedades: <Nombre de grupo de Active Directory>** en la que puede configurar el grupo seleccionado de Active Directory.

## Crear reglas para mover dispositivos a grupos de administración automáticamente

Puede configurar dispositivos para que se muevan automáticamente a grupos de administración luego de ser detectados durante un sondeo en una red empresarial.

*Para configurar reglas para mover automáticamente dispositivos a grupos de administración:*

1. En el árbol de consola, seleccione la carpeta **Dispositivos no asignados**.
2. En el espacio de trabajo de esta carpeta, haga clic en **Configurar reglas**.

   Esto abre la ventana **Propiedades: Dispositivos no asignados**. En la sección **Mover dispositivos**, configure las reglas para mover dispositivos a grupos de administración automáticamente.

La primera regla aplicable en la lista (del principio al final de la lista) se aplicará a un dispositivo.

## Usar el modo dinámico para la Infraestructura de escritorio virtual (VDI) en los dispositivos cliente

Es posible utilizar máquinas virtuales temporales para implementar una infraestructura virtual en una red corporativa. Kaspersky Security Center detecta las máquinas virtuales temporales y agrega información acerca de estas a la base de datos del Servidor de administración. Después de que un usuario termina de usar una máquina virtual temporal, esta máquina se elimina de la infraestructura virtual. Sin embargo, se puede guardar un registro sobre la máquina virtual eliminada en la base de datos del Servidor de administración. Además, las máquinas virtuales inexistentes se pueden visualizar en la Consola de administración.

Para evitar que se guarde información sobre máquinas virtuales inexistentes, Kaspersky Security Center admite el modo dinámico para la Infraestructura de Escritorio Virtual (VDI). El administrador puede habilitar la compatibilidad con el modo dinámico para VDI en las propiedades del paquete de instalación del Agente de red que se instalará en la máquina virtual temporal.

Cuando se deshabilita una máquina virtual temporal, el Agente de red notifica al Servidor de administración que la máquina se ha deshabilitado. Si la máquina virtual se ha deshabilitado correctamente, se la elimina de la lista de dispositivos conectados al Servidor de administración. Si la máquina virtual se deshabilita con errores y el Agente de red no envía una notificación sobre la máquina virtual deshabilitada al Servidor de administración, se usa un escenario de copia de seguridad. En este escenario, una máquina virtual se elimina de la lista de dispositivos conectados al Servidor de administración después de tres intentos fallidos de sincronización con el Servidor de administración.

## Habilitación del modo dinámico de la Infraestructura de escritorio virtual (VDI) en las propiedades de un paquete de instalación para el Agente de red

*Para habilitar el modo dinámico de la Infraestructura de escritorio virtual (VDI):*

1. En la carpeta **Instalación remota** del árbol de la consola, seleccione la subcarpeta **Paquetes de instalación**.
2. En el menú contextual del paquete de instalación del Agente de red, seleccione **Propiedades**.

   Se abre la ventana **Propiedades: Agente de red de Kaspersky Security Center**.
3. En la ventana **Propiedades: Agente de red de Kaspersky Security Center**, seleccione la sección **Avanzado**.
4. En la sección **Avanzado**, seleccione la opción **Habilitar modo dinámico para VDI**.

El dispositivo en el que se instalará el Agente de red formará parte de VDI.

## Buscar dispositivos que formen parte de la VDI

*Para buscar dispositivos no asignados que formen parte de la VDI:*

1. Seleccione **Buscar** en el menú contextual de la carpeta **Dispositivos no asignados**.

   Para ver una lista de todos los dispositivos que forman parte de la Infraestructura de escritorio virtual (VDI), en el menú contextual de la carpeta **Servidor de administración**, seleccione **Buscar**.
2. En la ventana **Buscar**, en la pestaña **Máquinas virtuales**, seleccione **Sí** en el grupo de configuración **Parte de la infraestructura de escritorio virtual**.
3. Haga clic en el botón **Buscar ahora**.

Se mostrará la lista de dispositivos no asignados que forman parte de la Infraestructura de escritorio virtual.

## Mover los dispositivos que forman parte de la VDI a un grupo de administración

*Para mover los dispositivos que formen parte de la VDI a un grupo de administración, realice lo siguiente:*

1. En el espacio de trabajo de la carpeta **Dispositivos no asignados**, haga clic en **Configurar reglas**.

   Se abre la ventana de propiedades de la carpeta **Dispositivos no asignados**.
2. En la ventana de propiedades de la carpeta **Dispositivos no asignados**, en la sección **Mover dispositivos**, haga clic en el botón **Agregar**.

   Se abre la ventana **Nueva regla**.
3. En la ventana **Nueva regla**, seleccione la sección **Máquinas virtuales**.
4. En la lista desplegable **Es una máquina virtual**, seleccione **Sí**.

Se creará una regla para la reubicación del dispositivo a un grupo de administración.

# Inventario de equipos

La lista de hardware (**Repositorios** → **Hardware**) que usa para hacer un inventario del equipamiento se completa de dos formas: automática y manualmente. Después de cada sondeo de la red, todos los dispositivos que se detectan se agregan a la lista automáticamente; sin embargo, también puede agregar los dispositivos de forma manual si no desea sondear la red. Puede agregar otros dispositivos a la lista de forma manual, como routers, impresoras o hardware del dispositivo.

En las propiedades de un dispositivo puede ver y editar información detallada acerca de ese dispositivo.

La lista de hardware puede incluir los siguientes tipos de dispositivos:

- Equipos
- Dispositivos móviles
- Dispositivos de red
- Dispositivos virtuales
- Componentes OEM
- Periféricos de equipos
- Dispositivos conectados
- Teléfonos de VoIP
- Repositorios de red

El administrador puede asignar el atributo de *Equipo de empresa* a los dispositivos detectados. Este atributo puede asignarse manualmente en las propiedades de un dispositivo o el administrador puede especificar los criterios para que los atributos se asignen automáticamente. En este caso, el atributo de *Equipo de empresa* se asigna por tipo de dispositivo.

Kaspersky Security Center permite cancelar equipos. Para hacer esto, seleccione la opción **Dispositivo cancelado** en las propiedades del dispositivo. Ese dispositivo no se muestra en la lista de equipos.

Un administrador puede administrar la lista de controladores lógicos programables (PLC) en la carpeta **Hardware**. Encontrará información detallada para administrar la lista de PLC en la *Guía para usuarios de Kaspersky Industrial Cyber Security for Nodes*.

## Agregar información sobre los dispositivos nuevos

*Para agregar información acerca de nuevos dispositivos en la red:*

1. En la carpeta **Repositorios** del árbol de consola, seleccione la subcarpeta **Hardware**.
2. En el espacio de trabajo de la carpeta **Hardware**, haga clic en el botón **Agregar dispositivo** para abrir la ventana **Nuevo dispositivo**.

   Se abre la ventana **Nuevo dispositivo**.

3. En la ventana **Nuevo dispositivo**, en la lista desplegable **Tipo**, seleccione un tipo de dispositivo que desee agregar.

4. Haga clic en **Aceptar**.

   La ventana de Propiedades del dispositivo se abre en la sección **General**.

5. En la sección **General** complete los campos de entrada con datos del dispositivo. La sección **General** detalla la siguiente configuración:

   - **Dispositivo de la empresa**. Seleccione esta casilla si desea asignarle el atributo *Empresa* al dispositivo. Mediante este atributo, puede buscar dispositivos en la carpeta **Hardware**.

   - **Dispositivo cancelado**. Seleccione esta casilla si no desea que el dispositivo figure en la lista de dispositivos de la carpeta **Hardware**.

6. Haga clic en **Aplicar**.

El nuevo dispositivo se mostrará en el espacio de trabajo de la carpeta **Hardware**.

## Configurar criterios usados para los dispositivos de empresa

*Para configurar los criterios de detección para los dispositivos de empresa:*

1. En la carpeta **Repositorios** del árbol de consola, seleccione la subcarpeta **Hardware**.

2. En el espacio de trabajo de la carpeta **Hardware**, haga clic en el botón **Acciones adicionales** y seleccione **Configurar regla para dispositivos de empresa** en la lista desplegable.

   Se abre la ventana de propiedades de hardware.

3. En la ventana de propiedades de hardware, en la sección **Dispositivos de empresa**, seleccione un método para asignar el atributo *Empresa* al dispositivo:

   - **Establecer el atributo de dispositivo de la empresa manualmente para el dispositivo**. El atributo *Hardware de empresa* se asigna manualmente al dispositivo en la ventana de propiedades del dispositivo en la sección **General**.

   - **Establecer el atributo del dispositivo de la empresa de forma automática**. En el bloque de configuración **Por tipo de dispositivo**, especifique los tipos de dispositivos a los que la aplicación asignará automáticamente el atributo *Empresa*.

     Esta opción afecta solo a los dispositivos agregados a través del sondeo de red. Para los dispositivos agregados manualmente, configure el atributo *Empresa* manualmente.

4. Haga clic en **Aceptar**.

Se configuran los criterios de detección para dispositivos empresariales.

## Configuración de campos personalizados

*Para configurar campos personalizados de dispositivos:*

1. En la carpeta **Repositorios** del árbol de consola, seleccione la subcarpeta **Hardware**.
2. En el espacio de trabajo de la carpeta **Hardware**, haga clic en el botón **Acciones adicionales** y seleccione **Configurar campos de datos personalizados** en la lista desplegable.

   Se abre la ventana de propiedades de hardware.
3. En la ventana de propiedades de hardware, seleccione la sección **Campos personalizados** y haga clic en el botón **Agregar**.

   Se abre la ventana **Agregar campo**.
4. En la ventana **Agregar campo**, especifique el nombre del campo personalizado que aparecerá en las propiedades del hardware.

   Puede crear múltiples campos personalizados con nombres únicos.
5. Haga clic en **Aceptar**.

Los campos personalizados que se han agregado se muestran en la sección **Campos personalizados** de las propiedades del hardware. Puede usar campos personalizados para proporcionar información específica sobre dispositivos. Por ejemplo, este podría ser el número de orden interno para una compra de hardware.

# Licencias

En esta sección encontrará información sobre los conceptos generales relacionados con la licencia de Kaspersky Security Center 15.1.

# Eventos sobre límites de licencia superados

Kaspersky Security Center le permite obtener información sobre eventos cuando las aplicaciones de Kaspersky instaladas en dispositivos cliente superan ciertos límites de licencia.

El nivel de importancia de estos eventos cuando se supera un límite de licencia se define según las siguientes reglas:

- Cuando se ha utilizado entre un 90 % y un 100 % del número total de unidades cubiertas por la licencia, el evento se publica con el nivel de importancia **Información**.
- Cuando se ha utilizado entre un 100 % y un 110 % del número total de unidades cubiertas por la licencia, el evento se publica con el nivel de importancia **Advertencia**.
- Cuando se ha utilizado más de un 110 % del número total de unidades cubiertas por la licencia, el evento se publica con el nivel de importancia **Evento crítico**.

# Sobre licencias

Esta sección contiene información sobre licencias de aplicaciones de Kaspersky administradas a través de Kaspersky Security Center.

## Acerca de la licencia

Una *licencia* otorga el derecho a usar Kaspersky Security Center por un tiempo limitado según las condiciones del Contrato de licencia firmado (Contrato de licencia de usuario final).

El alcance de los servicios y el período de validez dependen del tipo de licencia con el que se utiliza la aplicación.

Se proporcionan los siguientes tipos de licencia:

- *Prueba*

  Una licencia gratuita diseñada para probar la aplicación. Usualmente, una licencia de prueba tiene un plazo de vigencia breve.

  Cuando vence la licencia de prueba, todas las características de Kaspersky Security Center se deshabilitan. Para seguir usando la aplicación, se debe adquirir una licencia comercial.

  Puede usar la aplicación con una licencia de prueba solo durante un período de prueba.

- *Comercial*

  Una licencia pagada.

  Cuando caduca una licencia comercial, se deshabilitan las principales características de la aplicación. Para seguir usando Kaspersky Security Center, se debe renovar la licencia comercial. Una vez que caduca una licencia comercial, no puede seguir usando la aplicación y debe eliminarla de su dispositivo.

  Se recomienda renovar la licencia antes de que caduque para garantizar una protección ininterrumpida contra las amenazas a la seguridad.

## Acerca del Contrato de licencia de usuario final

El *Contrato de licencia de usuario final* (Contrato de licencia o EULA) es un acuerdo obligatorio entre AO Kaspersky Lab y usted que estipula los términos según los cuales puede utilizar la aplicación.

Lea detenidamente el Contrato de licencia antes de comenzar a utilizar la aplicación.

Kaspersky Security Center y sus componentes, por ejemplo, el Agente de red, tienen su propio EULA.

Puede ver los términos del Contrato de licencia de usuario final para Kaspersky Security Center utilizando los siguientes métodos:

- Durante la instalación de Kaspersky Security Center.
- Leyendo el documento license.txt incluido en el kit de distribución de Kaspersky Security Center.

- Leyendo el documento license.txt en la carpeta de instalación de Kaspersky Security Center.
- puede descargar el archivo license.txt desde el sitio web de Kaspersky.

Puede ver los términos del Contrato de licencia de usuario final para el Agente de red para Windows, el Agente de red para Mac y el Agente de red para Linux utilizando los siguientes métodos:

- Durante la descarga del paquete de distribución del Agente de red desde los servidores web de Kaspersky.
- Durante la instalación del Agente de red para Windows, el Agente de red para Mac o el Agente de red para Linux.
- Al leer el documento license.txt incluido en el paquete de distribución del Agente de red para Windows, el Agente de red para Mac o el Agente de red para Linux.
- Al leer el documento license.txt incluido en la carpeta de instalación del Agente de red para Windows, el Agente de red para Mac o el Agente de red para Linux.
- puede descargar el archivo license.txt desde el sitio web de Kaspersky.

Acepta los términos del Contrato de licencia de usuario final al confirmar que está de acuerdo con el Contrato de licencia de usuario final al instalar la aplicación. Si no acepta los términos del Contrato de licencia, cancele la instalación de la aplicación y no la utilice.

## Acerca del certificado de licencia

Un *certificado de licencia* es un documento que se entrega adjunto a un archivo de clave o código de activación.

El certificado de licencia contiene la siguiente información sobre la licencia proporcionada:

- Id. de la licencia o número de orden
- Información sobre el usuario al que se le ha otorgado la licencia
- Información sobre la aplicación que se puede activar con la licencia otorgada
- Límite al número de unidades con licencia (por ejemplo, el número de dispositivos en los que la licencia otorgada permite usar la aplicación)
- Fecha en que comienza la validez de la licencia
- Fecha de caducidad de la licencia o periodo de vigencia de la licencia
- Tipo de licencia

## Acerca de la clave de licencia

La *clave de licencia* es una secuencia de bits que se puede aplicar para activar y utilizar la aplicación de acuerdo con el Contrato de licencia de usuario final. Las claves de licencia son generadas por los especialistas de Kaspersky.

Puede agregar una clave de licencia a la aplicación mediante uno de los siguientes métodos: aplicando el *archivo de clave* o ingresando un *código de activación*. La clave de licencia se muestra en la interfaz de la aplicación como una secuencia alfanumérica única después de que la agrega a la aplicación.

Kaspersky puede bloquear la clave de licencia en caso de que se hayan infringido los términos del Contrato de licencia. Si la clave de licencia se ha bloqueado, debe agregar otra clave si desea usar la aplicación.

Una clave de licencia puede ser activa o adicional (de reserva).

Una *clave de licencia activa* es la clave que la aplicación está utilizando. Se puede agregar una clave de licencia activa para una licencia de prueba o comercial. La aplicación no puede tener más de una clave de licencia activa.

Una *clave de licencia adicional (o de reserva)* es una clave de licencia que le brinda a una persona el derecho a usar la aplicación, pero que no está activa en un momento dado. Una clave de licencia adicional se activa de forma automática cuando caduca la licencia asociada con la clave de licencia activa actual. Se puede agregar una clave de licencia adicional únicamente si ya se ha agregado una clave de licencia activa.

Se puede agregar una clave de licencia para la licencia de prueba como una clave de licencia activa. No se puede agregar una clave de licencia para la licencia de prueba como una clave de licencia adicional.

## Acerca del archivo de clave

El *archivo de clave* es un archivo con la extensión .key que le proporciona Kaspersky. Los archivos de claves están diseñados para activar la aplicación agregando una clave de licencia.

Recibirá un archivo de clave en la dirección de correo electrónico que proporcionó al comprar Kaspersky Security Center o al solicitar la versión de prueba de Kaspersky Security Center.

No es necesario conectarse a los servidores de activación de Kaspersky para activar la aplicación con un archivo de clave.

Puede restaurar un archivo de clave si se ha eliminado accidentalmente. Es posible que necesite un archivo de clave para registrar una cuenta de Kaspersky CompanyAccount, por ejemplo.

Para recuperar el archivo de clave, realice cualquiera de las siguientes acciones:

- Póngase en contacto con el vendedor de la licencia.
- Reciba un archivo de clave a través del sitio web de Kaspersky mediante su código de activación disponible.
- Exporte un archivo de clave de licencia desde otro Servidor de administración.

## Acerca de la suscripción

*Suscripción a Kaspersky Security Center* es una solicitud para usar la aplicación con las opciones seleccionadas (fecha de vencimiento de la suscripción, número de dispositivos protegidos). Puede registrar su suscripción a Kaspersky Security Center con su proveedor de servicios (por ejemplo, su proveedor de Internet). Una suscripción se puede renovar manualmente o automáticamente; también se puede cancelar.

Una suscripción puede ser limitada (puede tener un límite de un año, por ejemplo) o puede ser ilimitada, en cuyo caso no tendrá fecha de caducidad. Para continuar usando Kaspersky Security Center tras el vencimiento de una suscripción limitada, debe renovar la suscripción. Una suscripción ilimitada se renueva automáticamente si el proveedor de servicios ha recibido a término y por adelantado el pago correspondiente.

Cuando una suscripción limitada caduca, la aplicación puede seguir funcionando por un tiempo adicional, durante un período de gracia. Este período puede aprovecharse para renovar la suscripción. El proveedor de servicios define la disponibilidad y la duración del período de gracia.

Para usar Kaspersky Security Center con suscripción, debe aplicar el código de activación que le envía el proveedor de servicios.

Puede aplicar otro código de activación para Kaspersky Security Center únicamente después del vencimiento de la suscripción o cuando la cancela.

El conjunto de acciones disponibles para administrar una suscripción puede variar según el proveedor de servicios. Su proveedor de servicios podría no ofrecerle un período de gracia para renovar la suscripción; en tal caso, la aplicación dejará de funcionar.

Los códigos de activación adquiridos por suscripción no se pueden usar para activar versiones anteriores de Kaspersky Security Center.

Al usar la aplicación con suscripción, Kaspersky Security Center automáticamente intenta acceder al servidor de activación en los intervalos de tiempo especificados hasta el vencimiento de la suscripción. Esto garantiza que la información sobre la suscripción esté sincronizada con el servidor de activación. Si los servidores DNS configurados en el sistema no permiten acceder al servidor de Kaspersky, la aplicación utiliza servidores DNS públicos. Si necesita renovar su suscripción, puede hacerlo en el sitio web de su proveedor de servicios.

Puede actualizar la información sobre la suscripción manualmente, sin esperar a que Kaspersky Security Center acceda al servidor de activación. Por ejemplo, esto puede ser útil cuando cambie la configuración de la suscripción.

*Para actualizar la información sobre la suscripción manualmente, siga estos pasos:*

1. En el árbol de consola, seleccione la carpeta **Licencias de Kaspersky**.

2. Haga clic en **Acciones adicionales** y, en la lista desplegable, seleccione **Sincronizar la configuración de la suscripción con el servidor de licencias**.

La información sobre la suscripción se actualiza en el servidor de activación.

## Acerca del código de activación

Un *código de activación* es una secuencia única formada por 20 caracteres alfanuméricos. Se ingresa un código de activación para agregar una clave de licencia que activa Kaspersky Security Center. El código de activación se recibe en la dirección de correo electrónico que se especificó, después de adquirir Kaspersky Security Center o después de solicitar una versión de prueba de Kaspersky Security Center.

Para activar la aplicación mediante el código de activación, necesita acceso a Internet para establecer la conexión con los servidores de activación de Kaspersky. Si los servidores DNS configurados en el sistema no permiten acceder a los servidores de Kaspersky, la aplicación utiliza servidores DNS públicos.

En algunos casos, cuando se ha utilizado un código de activación para activarla, la aplicación se contactará periódicamente con los servidores de activación de Kaspersky a fin de determinar el estado de la clave de licencia. Debe brindarle acceso a Internet a la aplicación para permitir estas comprobaciones.

Si perdió su código de activación después de instalar la aplicación, comuníquese con el socio de Kaspersky a quien le compró la licencia.

Las aplicaciones administradas no se pueden activar utilizando archivos de clave: solo se aceptan códigos de activación.

## Revocar la aceptación de un Contrato de licencia de usuario final

Si decide detener la protección de sus dispositivos cliente, puede desinstalar las aplicaciones de Kaspersky administradas y revocar el Contrato de licencia de usuario final (EULA) para estas aplicaciones.

*Para revocar un EULA vinculado a una aplicación de Kaspersky administrada:*

1. En el árbol de la consola, seleccione **Servidor de administración → Avanzado → EULA aceptados**.

   Se muestra una lista con los EULA aceptados tras la creación de paquetes de instalación, la instalación sin problemas de actualizaciones o el despliegue de Kaspersky Security para dispositivos móviles.

2. En la lista, seleccione el EULA que desee revocar.

   Puede ver las siguientes propiedades del EULA:

   - Fecha en que se aceptó el EULA.
   - El nombre del usuario que aceptó el EULA.
   - Enlace a los términos del EULA.
   - Lista de los objetos que están conectados al EULA: nombres de los paquetes de instalación, nombres de las actualizaciones integradas, nombres de las aplicaciones móviles.

3. Haga clic en el botón **Revocar EULA**.

   En la ventana que se abre, se le informa que debe desinstalar la aplicación Kaspersky correspondiente al EULA.

4. Haga clic en el botón para confirmar la revocación.

   Kaspersky Security Center verifica si los paquetes de instalación (correspondientes a la aplicación de Kaspersky administrada cuyo EULA desea revocar) se han eliminado.

   Para revocar el EULA de una aplicación de Kaspersky administrada, los paquetes de instalación de la misma deben haberse eliminado.

Se revoca el EULA. No se muestra en la lista de EULA en la sección **Servidor de administración → Avanzado → EULA aceptados**. Si revoca el EULA de una aplicación de Kaspersky, no podrá utilizarla para proteger sus dispositivos cliente.

# Sobre la provisión de datos

## Datos transferidos a terceros

Al usar la función Administración de dispositivos móviles del Software, con el fin de hacer llegar oportunamente a través del mecanismo de notificación automática los comandos a los dispositivos que ejecutan el sistema operativo Android, se utiliza Google Firebase Cloud Messaging. Si el usuario ha configurado el uso del servicio Google Firebase Cloud Messaging, el usuario acepta proporcionar la siguiente información al servicio Google Firebase Cloud Messaging en modo automático: los id. de instalación de las aplicaciones Kaspersky Endpoint Security para Android a las que deban enviarse notificaciones push.

Para que no se intercambie información con el servicio Google Firebase Cloud Messaging, el usuario debe revertir la configuración de uso del servicio Google Firebase Cloud Messaging.

Cuando se usa la característica de administración de dispositivos móviles del software, se usa también el servicio Apple Push Notification Service (APNs) con el fin de que los comandos transmitidos a través del mecanismo de notificación push lleguen sin dilaciones a los dispositivos que ejecutan el sistema operativo iOS. Si el usuario ha instalado un certificado de APNs en un servidor de MDM para iOS, ha creado un perfil de MDM para iOS con una colección de ajustes para conectar dispositivos móviles iOS al software y ha instalado dicho perfil en sus dispositivos móviles, el usuario acepta proporcionar la siguiente información a APNs en modo automático:

- Token: token del dispositivo para notificaciones push. El servidor usa este token cuando envía notificaciones push al dispositivo.
- PushMagic: cadena que debe incluirse en la notificación push. El valor de la cadena es generado por el dispositivo.

## Datos procesados localmente

Kaspersky Security Center está diseñado para ejecutar tareas de administración y mantenimiento básicas en la red de una organización de forma centralizada. Kaspersky Security Center le brinda al administrador acceso a información detallada sobre el nivel de seguridad de la red de la organización y le permite configurar todos los componentes de un sistema de protección basado en las aplicaciones de Kaspersky. Estas son las principales funciones que se pueden realizar a través de Kaspersky Security Center:

- Detectar dispositivos, y a los usuarios de esos dispositivos, en la red de la organización
- Crear una jerarquía de grupos de administración para la administración de dispositivos
- Instalar aplicaciones de Kaspersky en los dispositivos
- Administrar la configuración y las tareas de las aplicaciones instaladas
- Administrar actualizaciones para las aplicaciones desarrolladas por Kaspersky y por otras empresas, así como encontrar y reparar vulnerabilidades
- Activar las aplicaciones de Kaspersky en los dispositivos
- Administrar cuentas de usuario

- Ver información sobre el funcionamiento de las aplicaciones de Kaspersky en los dispositivos
- Ver informes

Para permitir estas funciones, Kaspersky Security Center puede recibir, almacenar y procesar la siguiente información:

- Información sobre los dispositivos en la red de la organización recibida mediante el análisis del dominio de Windows, Active Directory o controladores de dominio de Samba, o mediante el análisis de intervalos de IP. El Servidor de administración obtiene datos de forma independiente o recibe datos del Agente de red como punto de distribución.
- Información de Active Directory y Samba sobre unidades organizativas, dominios, usuarios y grupos. El Servidor de administración obtiene datos de forma independiente o recibe datos del Agente de red como punto de distribución.
- Detalles de los dispositivos administrados. El Agente de red transfiere los datos que se muestran a continuación de los dispositivos al Servidor de administración. El usuario ingresa el nombre y la descripción del dispositivo en la interfaz de la Consola de administración o en la interfaz de Kaspersky Security Center Web Console:
    - Especificaciones técnicas del dispositivo administrado y de sus componentes, que son necesarias para identificar el dispositivo: nombre y descripción del dispositivo; nombre y tipo de dominio de Windows; nombre del dispositivo en el entorno de Windows; dominio DNS y nombre DNS; dirección IPv4; dirección IPv6; ubicación de red; dirección MAC; número de serie; tipo de sistema operativo; indicación de si el dispositivo es una máquina virtual y tipo de hipervisor; e indicación de si el dispositivo es una máquina virtual dinámica que forma parte de una VDI.
    - Otras especificaciones de los dispositivos administrados y de sus componentes necesarias para auditar los dispositivos administrados y para tomar decisiones sobre si ciertos parches y actualizaciones deben aplicarse: estado del Agente de Windows Update (WUA); arquitectura del sistema operativo; proveedor del sistema operativo; número de compilación del sistema operativo; id. de versión del sistema operativo; carpeta de ubicación del sistema operativo; si el dispositivo es una máquina virtual, el tipo de máquina virtual; nombre del Servidor de administración virtual que administra el dispositivo; datos del dispositivo de nube (región de la nube, VPC, zona de disponibilidad en la nube, subred de nube, zona de ubicación en la nube).
    - Detalles de acciones realizadas en los dispositivos administrados: fecha y hora de la última actualización; hora en que el dispositivo estuvo visible por última vez en la red; estado de espera de reinicio; hora en que se encendió el dispositivo.
    - Detalles de las cuentas de usuario del dispositivo y de sus sesiones de trabajo.
- Datos recibidos al ejecutar diagnósticos remotos en un dispositivo administrado: archivos de seguimiento, información del sistema, detalles de las aplicaciones de Kaspersky instaladas en el dispositivo, archivos de volcado, registros de eventos, los resultados de la ejecución de los scripts de diagnóstico recibidos del Servicio de soporte técnico de Kaspersky.
- Estadísticas de funcionamiento del punto de distribución, si el dispositivo es un punto de distribución. El Agente de red transfiere datos del dispositivo al Servidor de administración.
- Configuración del punto de distribución ingresada por el usuario en la Consola de administración o en Kaspersky Security Center Web Console.
- Datos necesarios para conectar dispositivos móviles al Servidor de administración: certificado, puerto de conexión móvil, dirección de conexión del Servidor de administración. El usuario ingresa los datos en la Consola de administración o en Kaspersky Security Center Web Console.

- Detalles de los dispositivos móviles transferidos mediante el protocolo de MDM para iOS. Los datos detallados a continuación se transfieren del dispositivo móvil al Servidor de administración:

  - Especificaciones técnicas del dispositivo móvil y de sus componentes necesarias para identificar el dispositivo: nombre del dispositivo; modelo; nombre y número de compilación del sistema operativo; número de modelo del dispositivo; número de IMEI; UDID; MEID; número de serie; cantidad de memoria; versión del firmware del módem; dirección MAC de Bluetooth; dirección MAC de Wi-Fi; detalles de la tarjeta SIM (el ICCID, como parte del id. de la tarjeta SIM).

  - Detalles de la red móvil utilizada por el dispositivo administrado: tipo de red móvil, nombre de la red móvil que se está utilizando, nombre de la red móvil doméstica, versión de la configuración del operador de red móvil, estado del roaming de voz, estado del roaming de datos, código de país de la red doméstica, código del país de residencia, código de la red que se está utilizando y nivel de cifrado.

  - Configuración de seguridad del dispositivo móvil: uso de contraseña, conformidad de la contraseña con los requisitos impuestos por directiva, lista de perfiles de configuración y lista de perfiles de aprovisionamiento utilizados para la instalación de aplicaciones de terceros.

  - Fecha de la última sincronización con el Servidor de administración y estado de administración del dispositivo.

- Detalles de las aplicaciones de Kaspersky instaladas en el dispositivo. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red:

  - Configuración de las aplicaciones de Kaspersky instaladas en el dispositivo administrado: nombre y versión de la aplicación de Kaspersky; estado; estado de la protección en tiempo real; fecha y hora del último análisis del dispositivo; número de amenazas detectadas; número de objetos que no se pudieron desinfectar; disponibilidad y estado de los componentes de la aplicación; versión de las bases de datos antivirus y hora en que se actualizaron por última vez; detalles de la configuración y las tareas de las aplicaciones de Kaspersky; información sobre las claves de licencia activa y de reserva; id. y fecha de instalación de la aplicación.

  - Estadísticas de funcionamiento de cada aplicación: eventos relacionados con los cambios en el estado de los componentes de la aplicación de Kaspersky en el dispositivo administrado y con el desempeño de las tareas iniciadas por los componentes de la aplicación.

  - Estado del dispositivo definido por la aplicación de Kaspersky.

  - Etiquetas asignadas por la aplicación de Kaspersky.

  - Conjunto de actualizaciones instaladas y aplicables para la aplicación de Kaspersky.

- Datos contenidos en los eventos de los componentes de Kaspersky Security Center y en los de las aplicaciones de Kaspersky administradas. El Agente de red transfiere datos del dispositivo al Servidor de administración.

- Datos necesarios para la integración de Kaspersky Security Center con un sistema SIEM para la exportación de eventos. El usuario ingresa los datos en la Consola de administración o en Kaspersky Security Center Web Console.

- Configuración de los componentes de Kaspersky Security Center y de las aplicaciones de Kaspersky administradas definida en las directivas y en los perfiles de las directivas. El usuario ingresa datos en la Consola de administración o en la interfaz de Kaspersky Security Center Web Console.

- Configuración de las tareas para los componentes de Kaspersky Security Center y para las aplicaciones de Kaspersky administradas. El usuario ingresa datos en la Consola de administración o en la interfaz de Kaspersky Security Center Web Console.

- Datos tratados por la característica Administración de vulnerabilidades y parches. El Agente de red transfiere los datos que se indican a continuación del dispositivo al Servidor de administración:
  - Detalles de las aplicaciones y de los parches instalados en los dispositivos administrados (Registro de aplicaciones).
  - Información sobre el hardware detectado en los dispositivos administrados (Registro de hardware).

    Si el Agente de red está instalado en un dispositivo con Windows, envía al Servidor de administración la siguiente información sobre el hardware del dispositivo:
    - RAM
    - Dispositivos de almacenamiento
    - Placa madre
    - CPU
    - Adaptadores de red
    - Monitores
    - Adaptador de video
    - Tarjeta de sonido

    Si el Agente de red está instalado en un dispositivo con Linux o macOS, envía al Servidor de administración la siguiente información sobre el hardware del dispositivo, si el sistema operativo la proporciona:
    - Volumen total de la RAM
    - Volumen total de los dispositivos de almacenamiento masivo
    - Placa madre
    - CPU
    - Adaptadores de red
  - Detalles de las vulnerabilidades presentes en el software de terceros detectado en los dispositivos administrados.
  - Detalles de las actualizaciones disponibles para las aplicaciones de terceros instaladas en los dispositivos administrados.
  - Detalles de las actualizaciones de Microsoft encontradas por la función WSUS.
  - Lista de las actualizaciones de Microsoft encontradas por la función WSUS que se deben instalar en el dispositivo.
- Datos necesarios para descargar actualizaciones en un Servidor de administración aislado a fin de reparar vulnerabilidades en el software de terceros instalado en los dispositivos administrados. El usuario introduce y transmite datos mediante la utilidad klscflag del Servidor de administración.

- Datos necesarios para el funcionamiento de Kaspersky Security Center con los entornos de nube (Amazon Web Services, Microsoft Azure, Google Cloud, Yandex Cloud). El usuario ingresa los datos en la Consola de administración o en Kaspersky Security Center Web Console.

- Categorías de aplicaciones creadas por el usuario. El usuario ingresa datos en la Consola de administración o en la interfaz de Kaspersky Security Center Web Console.

- Detalles de los archivos ejecutables detectados por la función Control de aplicaciones en los dispositivos administrados. El usuario ingresa datos en la Consola de administración o en la interfaz de Kaspersky Security Center Web Console. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.

- Detalles de los archivos almacenados en Copia de seguridad. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.

- Detalles de los archivos puestos en cuarentena. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.

- Detalles de los archivos solicitados por los especialistas de Kaspersky para un análisis detallado. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.

- Detalles del estado y la activación de las reglas del Control de anomalías adaptativo. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.

- Información sobre los dispositivos (unidades de memoria, herramientas de transferencia de información, herramientas para copias de información impresas y buses de conexión) que se han instalado en el dispositivo administrado o que se han conectado a este y que fueron detectados por la función Control de dispositivos. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.

- Información sobre los dispositivos cifrados y el estado del cifrado. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red.

- Detalles de los errores de cifrado de datos registrados en dispositivos en los que se haya utilizado la función de cifrado de datos de las aplicaciones de Kaspersky. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.

- Lista de los controladores de lógica programable (PLC) administrados. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.

- Datos necesarios para la creación de una cadena de desarrollo de amenazas. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.

- Información sobre los intentos de los empleados de una organización de acceder a los servicios en la nube. La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red. Encontrará una lista con todos los datos en los archivos de ayuda de la aplicación correspondiente.

- Datos necesarios para la integración de Kaspersky Security Center con el servicio Kaspersky Managed Detection and Response (en Kaspersky Security Center Web Console, debe instalarse un complemento dedicado): token de inicio de integración, token de integración y token de sesión de usuario. El usuario ingresa el token de inicio de integración en la interfaz de Kaspersky Security Center Web Console. El servicio Kaspersky MDR transfiere el token de integración y el token de sesión de usuario a través del complemento dedicado.

- Detalles de los códigos de activación ingresados o los archivos de clave especificados. El usuario ingresa datos en la Consola de administración o en la interfaz de Kaspersky Security Center Web Console.

- Cuentas de usuario: nombre, descripción, nombre completo, dirección de correo electrónico, número de teléfono principal, contraseña, clave secreta generada por el Servidor de administración y contraseña de un solo uso para la verificación en dos pasos. El usuario ingresa datos en la Consola de administración o en la interfaz de Kaspersky Security Center Web Console.

- Datos que Identity and Access Manager necesita para ofrecer autenticación centralizada y permitir el inicio de sesión único (SSO) en las aplicaciones de Kaspersky integradas con Kaspersky Security Center: parámetros de instalación y configuración de Identity and Access Manager, sesión de usuario de Identity and Access Manager, tokens de Identity and Access Manager, estados de la aplicación cliente y estados del servidor de recursos. El usuario ingresa datos en la Consola de administración o en la interfaz de Kaspersky Security Center Web Console.

- Historial de revisiones de los objetos de administración. El usuario ingresa datos en la Consola de administración o en la interfaz de Kaspersky Security Center Web Console.

- Dirección IP del dispositivo en el que un usuario creó una revisión. El Servidor de administración define la dirección IP automáticamente.

- Registro de objetos de administración eliminados. El usuario ingresa datos en la Consola de administración o en la interfaz de Kaspersky Security Center Web Console.

- Paquetes de instalación creados a partir del archivo y ajustes de instalación. El usuario ingresa datos en la Consola de administración o en la interfaz de Kaspersky Security Center Web Console.

- Datos necesarios para mostrar comunicaciones emitidas por Kaspersky en Kaspersky Security Center Web Console. El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.

- Datos que se necesitan para el funcionamiento de los complementos de las aplicaciones administradas en Kaspersky Security Center Web Console y que han sido almacenados por estos complementos en la base de datos del Servidor de administración como parte de sus operaciones de rutina. Encontrará una descripción de los datos y los modos de proporcionarlos en los archivos de ayuda de la aplicación correspondiente.

- Ajustes definidos por el usuario en Kaspersky Security Center Web Console: idioma de localización y tema de la interfaz; ajustes de visualización del panel Supervisión; información sobre el estado de las notificaciones (Leídas / Por leer); estado de las columnas en las hojas de cálculo (Mostrar/Ocultar); progreso en el modo de capacitación. El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.

- Registro de eventos de Kaspersky para los componentes de Kaspersky Security Center y las aplicaciones de Kaspersky administradas. El registro de eventos de Kaspersky se almacena en cada dispositivo y nunca se transfiere al Servidor de administración.

- Certificado utilizado para establecer una conexión segura entre los dispositivos administrados y los componentes de Kaspersky Security Center. El usuario ingresa datos mediante la utilidad klsetsrvcert del Servidor de administración.

- Certificados para establecer la confianza en los recursos web internos de la organización. El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.

- Datos necesarios para el funcionamiento de Kaspersky Security Center en entornos de nube, como Amazon Web Services (AWS), Microsoft Azure, Google Cloud y Yandex.Cloud. El Servidor de administración recibe los datos de la máquina virtual en la que se ejecuta.
- Información sobre la aceptación por parte del usuario de los términos y condiciones de los contratos legales con Kaspersky.
- Los datos del Servidor de administración que el usuario ingresa en los siguientes componentes:
  - Consola de administración
  - Kaspersky Security Center Web Console
  - Terminal de línea de comandos cuando se usa la utilidad klscflag
  - Componentes que interactúan con el Servidor de administración a través de objetos de automatización de klakaut y de la interfaz OpenAPI de Kaspersky Security Center
- Cualquier dato que el usuario ingresa en la Consola de administración o en la interfaz de la Kaspersky Security Center Web Console.

Los datos detallados arriba pueden estar presentes en Kaspersky Security Center si se aplica uno de los siguientes métodos:

- El usuario ingresa datos en la interfaz de los siguientes componentes:
  - Consola de administración
  - Kaspersky Security Center Web Console
  - Terminal de línea de comandos cuando se usa la utilidad klscflag
  - Componentes que interactúan con el Servidor de administración a través de objetos de automatización de klakaut y de la interfaz OpenAPI de Kaspersky Security Center
- El Agente de red recibe los datos automáticamente desde el dispositivo y los transfiere al Servidor de administración.
- El Agente de red recibe los datos recuperados por la aplicación de Kaspersky administrada y los transfiere al Servidor de administración. Encontrará las listas de datos procesados por las aplicaciones de Kaspersky administradas en los archivos de ayuda de las aplicaciones correspondientes.
- El Servidor de administración obtiene información sobre los dispositivos en red de forma independiente o recibe información de un Agente de red que actúa como punto de distribución.
- Los datos se transfieren del dispositivo móvil al Servidor de administración mediante el protocolo MDM para iOS.

Los datos detallados se almacenan en la base de datos del Servidor de administración. Los nombres de usuario y las contraseñas se almacenan de forma cifrada.

Todos los datos detallados arriba pueden transferirse a Kaspersky solo a través de archivos de volcado, archivos de seguimiento o archivos de registro de los componentes de Kaspersky Security Center (entre estos, archivos de registro creados por utilidades o programas de instalación).

Los archivos de volcado, los archivos de seguimiento y los archivos de registro de los componentes de Kaspersky Security Center contienen datos aleatorios del Servidor de administración, del Agente de red, de la Consola de administración, del Servidor de MDM para iOS y de Kaspersky Security Center Web Console. Estos archivos pueden contener datos personales y confidenciales. Los archivos de volcado, los archivos de seguimiento y los archivos de registro se almacenan en el dispositivo de forma no cifrada. Los archivos de volcado, los archivos de seguimiento y los archivos de registro no se transfieren a Kaspersky automáticamente; sin embargo, el administrador puede transferir datos a Kaspersky manualmente a pedido del servicio de soporte técnico para resolver problemas con el funcionamiento de Kaspersky Security Center.

Al seguir los vínculos de la Consola de administración o de Kaspersky Security Center Web Console, el usuario da su consentimiento para que los siguientes datos se transfieran en forma automática:

- Código de Kaspersky Security Center
- Versión de Kaspersky Security Center
- Localización de Kaspersky Security Center
- Id. de licencia
- Tipo de licencia
- Indicación de si la licencia se compró a través de un socio

La lista de datos que se proporcionan a través de cada vínculo depende de la finalidad y la ubicación del vínculo.

Kaspersky utiliza los datos recibidos en forma anónima y solo con fines estadísticos generales. La información recibida se utiliza para generar estadísticas de resumen, que no contienen ningún tipo de dato personal o confidencial. Según se acumulan nuevos datos, se borran los datos más antiguos (una vez al año). Las estadísticas de resumen se almacenan indefinidamente.

Kaspersky protege toda la información que recibe según las exigencias de la ley y según las reglas de Kaspersky pertinentes. Los datos se transmiten a través de un canal seguro.

# Opciones de licencias de Kaspersky Security Center

Kaspersky Security Center puede funcionar en los siguientes modos:

- **Sin licencia (funcionalidad básica)**

  Kaspersky Security Center funciona en este modo antes de que se active la aplicación o después de que caduca la licencia comercial. Kaspersky Security Center con el soporte de la funcionalidad básica de la Consola de administración se entrega como una parte de las aplicaciones de Kaspersky para la protección de redes corporativas. También se puede descargar desde el sitio web de Kaspersky.

- **Licencia comercial**

  Si necesita una funcionalidad adicional que no esté incluida en la funcionalidad básica de la Consola de administración, debe comprar una licencia comercial.

  Cuando agregue una clave de licencia en la ventana de propiedades del Servidor de administración, verifique que esta le permita utilizar Kaspersky Security Center. Encontrará información a tal efecto en el sitio web de Kaspersky. La página web de cada solución contiene una lista de las aplicaciones que incluye. El Servidor de administración puede aceptar claves de licencia no admitidas (por ejemplo, una clave de licencia para Kaspersky Endpoint Security Cloud), pero esas claves de licencia no proporcionan nuevas funciones además de la funcionalidad básica de la Consola de administración.

| Característica o propiedad | Modo de funcionamiento de Kaspersky Security Center | |
|---|---|---|
| | Sin licencia | Licencia comercial |
| Funcionalidad básica de la Consola de administración<br><br>Están disponibles las siguientes funciones:<br>• Creación de Servidores de administración virtuales para administrar una red de oficinas remotas u organizaciones cliente.<br>• Creación de una jerarquía de grupos de administración para administrar dispositivos específicos como una única entidad.<br>• Instalación remota de aplicaciones.<br>• La configuración centralizada de aplicaciones instaladas en dispositivos cliente.<br>• Control del estado de la seguridad antivirus de una organización.<br>• Administración de roles de usuario.<br>• Estadísticas e informes sobre el funcionamiento de la aplicación, así como notificaciones sobre eventos críticos.<br>• Operaciones centralizadas con archivos que se movieron a la cuarentena o copia de seguridad y archivos cuyo procesamiento se ha pospuesto.<br>• Administración de la protección y el cifrado de datos.<br>• Enumeración y modificación de los grupos de aplicaciones con licencia existentes.<br>• Visualización y edición manual de la lista de componentes de hardware que detectó el sondeo de la red.<br>• Visualización de la lista de imágenes de sistema operativo disponibles para la instalación remota. | ✓ | ✓ |
| Administración de vulnerabilidades y parches: funcionalidad básica | ✓ | ✓ |

| Característica o propiedad | Modo de funcionamiento de Kaspersky Security Center | |
|---|---|---|
| | Sin licencia | Licencia comercial |
| Las siguientes tareas no requieren una licencia comercial:<br>• La tarea *Buscar vulnerabilidades y actualizaciones requeridas*<br>Mediante esta tarea, Kaspersky Security Center recibe las listas de las vulnerabilidades detectadas y las actualizaciones necesarias para el software de terceros instalado en los dispositivos administrados.<br>• La tarea *Instalar actualizaciones de Windows Update*<br>Esta tarea solo puede usarse para instalar actualizaciones de Windows Update. Para utilizar esta tarea, debe especificar manualmente las actualizaciones necesarias en la configuración de la tarea.<br>• La tarea *Reparar vulnerabilidades*<br>La tarea *Reparar vulnerabilidades* utiliza correcciones recomendadas para el software de Microsoft y correcciones de usuario para software de terceros. Para usar esta tarea, debe especificar manualmente las correcciones de usuario para las vulnerabilidades en la configuración de la tarea. | | |
| Administración de vulnerabilidades y parches: funcionalidad avanzada<br>Están disponibles las siguientes funciones:<br>• Instalación remota de actualizaciones de software y reparación de vulnerabilidades de forma automática, de acuerdo con las reglas que defina.<br>• Uso del Servidor de administración como servidor de Windows Server Update Services (WSUS) para proporcionar actualizaciones a los servicios de Windows Update en dispositivos en modo centralizado y con la frecuencia establecida. | — | ✓ |

| Característica o propiedad | Modo de funcionamiento de Kaspersky Security Center | |
|---|---|---|
| | Sin licencia | Licencia comercial |
| Función de administración de dispositivos móviles en la Consola de administración basada en MMC<br><br>La función de Administración de dispositivos móviles se utiliza para administrar dispositivos móviles MDM para iOS y Android.<br><br>Las siguientes funciones están disponibles para los dispositivos MDM con iOS:<br>• Poner nuevos dispositivos bajo la administración de Kaspersky Security Center.<br>• Creación y edición de perfiles de configuración, e instalación de perfiles de configuración en dispositivos móviles.<br>• Instalación de aplicaciones en dispositivos móviles, ya sea a través de App Store® o mediante archivos de manifiesto (.plist) o paquetes de instalación para dispositivos móviles (.ipa).<br>• Ejecución de comandos en dispositivos MDM con iOS, como el bloqueo de dispositivos móviles, el restablecimiento de la contraseña del dispositivo móvil y la eliminación de todos los datos del dispositivo móvil.<br><br>Las siguientes funciones están disponibles para dispositivos Android:<br>• Poner nuevos dispositivos bajo la administración de Kaspersky Security Center.<br>• Administrar Kaspersky Endpoint Security para Android mediante una directiva.<br>• Ejecutar comandos en dispositivos.<br><br>La unidad de administración para la Administración de dispositivos móviles es un dispositivo móvil. Un dispositivo móvil se considera administrado desde que se conecta a un servidor de dispositivos móviles. | — | ✓ (Se debe agregar una clave de licencia a las propiedades del Servidor de administración). |
| Protección de dispositivos móviles en Kaspersky Security Center Web Console<br><br>Kaspersky Security Center Web Console ofrece las siguientes funciones para administrar dispositivos móviles Android e iOS:<br>• Poner nuevos dispositivos bajo la administración de Kaspersky Security Center.<br>• Administrar Kaspersky Endpoint Security para Android y Kaspersky Security para iOS a través de directivas.<br>• Enviar comandos a los dispositivos móviles a través de los protocolos relevantes y ejecutar los comandos. | — | ✓ (Se debe agregar una clave de licencia en cada dispositivo móvil). |

| Característica o propiedad | Modo de funcionamiento de Kaspersky Security Center | |
|---|---|---|
| | Sin licencia | Licencia comercial |
| Administración de sistemas<br><br>Están disponibles las siguientes funciones:<br><br>• Instalación de sistemas operativos y aplicaciones.<br>Kaspersky Security Center permite crear imágenes de los sistemas operativos e instalarlas de forma remota en los dispositivos cliente de la red. También permite realizar instalaciones remotas de aplicaciones de Kaspersky o de otros proveedores. Puede capturar imágenes de los sistemas operativos de los dispositivos y transferir esas imágenes al Servidor de administración. Estas imágenes de los sistemas operativos se almacenan en el Servidor de administración, en una carpeta dedicada. Se captura y crea la imagen del sistema operativo de un dispositivo de referencia mediante una tarea de creación del paquete de instalación. Puede usar las imágenes recibidas para instalarlas en dispositivos de la red que aún no cuenten con un sistema operativo. En este caso se utiliza una tecnología denominada Preboot eXecution Environment (PXE).<br><br>• Administración del grupo de aplicaciones con licencia.<br><br>• Permiso remoto de conexión a dispositivos cliente a través de un componente de Microsoft® Windows® llamado Conexión a escritorio remoto.<br><br>• Conexión remota con dispositivos cliente mediante Windows Desktop Sharing.<br><br>• Conexión remota mediante **Visor de sesiones del escritorio remoto de Kaspersky**. | — | ✓ |

| Característica o propiedad | Modo de funcionamiento de Kaspersky Security Center | |
|---|---|---|
| | Sin licencia | Licencia comercial |
| Integración en entornos de nube<br>Kaspersky Security Center no solo funciona con dispositivos locales, sino que también proporciona características especiales para trabajar en un entorno de nube, como el Asistente de configuración del entorno de nube. Kaspersky Security Center funciona con las siguientes máquinas virtuales:<br>• Instancias de Amazon EC2<br>• Máquinas virtuales de Microsoft Azure<br>• Instancias de máquinas virtuales de Google Cloud<br>• Máquinas virtuales Yandex.Cloud | — | ✓ |
| Exportar eventos a un sistema SIEM a través del protocolo Syslog.<br>Usando el protocolo de Syslog, puede transmitir cualquier evento que ocurra en el Servidor de administración de Kaspersky Security Center y en Aplicaciones de Kaspersky instaladas en dispositivos administrados. El protocolo de Syslog es un protocolo de registro de mensajes estándares. Puede utilizarlo para exportar eventos a cualquier sistema SIEM. | ✓ | ✓ |

# Funciones de licencia de Kaspersky Security Center y aplicaciones administradas

La aplicación de licencias del Servidor de administración y de las aplicaciones administradas involucra lo siguiente:

- Puede agregar una clave de licencia o un código de activación válido a un Servidor de administración para activar la Administración de vulnerabilidades y parches, la Administración de dispositivos móviles o la Integración con los sistemas SIEM. Algunas funciones de Kaspersky Security Center solo son accesibles según los archivos de claves activa o los códigos de activación válidos agregados al Servidor de administración.
- Puede agregar varios archivos de clave y códigos de activación para aplicaciones administradas al repositorio del Servidor de administración.

## Sobre las licencias de Kaspersky Security Center

Si ha activado una de las funciones de la licencia (por, ejemplo, la Administración de dispositivos móviles) con un archivo de clave pero también desea usar función de la licencia (por ejemplo, la Administración de vulnerabilidades y parches), debe comprarle a su proveedor de servicios una archivo de clave que active ambas funciones y debe activar el Servidor de administración con esta archivo de clave.

### Funciones de licencia de aplicaciones administradas

Para obtener las licencias de las aplicaciones administradas, puede desplegar automáticamente (o de cualquier forma que le resulte cómoda) un archivo de clave o un código de activación. Puede usar los siguientes métodos para desplegar un código de activación o archivo de clave:

- Despliegue automático

  Si usa diferentes aplicaciones administradas y tiene que desplegar un archivo de clave o un código de activación específicos en los dispositivos, opte por otras formas de desplegar ese código de activación o archivo de clave.

  Kaspersky Security Center le permite desplegar las claves de licencia disponibles a los dispositivos automáticamente. Suponga, por ejemplo, que tiene tres claves de licencia en el repositorio del Servidor de administración. Ha seleccionado la casilla de verificación **Distribuir la clave de licencia automáticamente a los dispositivos administrados** para las tres claves de licencia. Los dispositivos de su organización tienen instalada una aplicación de seguridad de Kaspersky (por ejemplo, Kaspersky Endpoint Security para Windows). Se detecta un nuevo dispositivo al que se debe desplegar una clave de licencia. La aplicación determina, por ejemplo, que dos de las claves de licencia del repositorio se pueden aplicar al dispositivo: una clave de licencia llamada *Key_1* y una clave de licencia llamada *Key_2*. Una de estas claves de licencia se despliega al dispositivo. En este caso, no se puede predecir cuál de las dos claves de licencia se desplegará en el dispositivo porque el despliegue automático de claves de licencia no proporciona ninguna actividad de administrador.

  Cuando se despliega una clave de licencia, los dispositivos se vuelven a contar para esa clave de licencia. Debe asegurarse de que la cantidad de dispositivos a los que se desplegó la clave de licencia no exceda el límite de la licencia. Si la cantidad de dispositivos excede el límite de la licencia, a todos los dispositivos que no estaban cubiertos por la licencia se les asignará el estado *Crítico*.

- Adición de un archivo de clave o un código de activación al paquete de instalación de una aplicación administrada

  Si instala una aplicación administrada con un paquete de instalación, puede especificar un código de activación o un archivo de clave en este paquete de instalación o en la directiva de la aplicación. En ese caso, la clave de licencia se desplegará a los dispositivos administrados cuando estos se sincronicen nuevamente con el Servidor de administración.

- Despliegue con la tarea Agregar clave de licencia para una aplicación administrada

  Si opta por usar la tarea Agregar clave de licencia para una aplicación administrada, puede seleccionar la clave que debe desplegarse a los dispositivos y seleccionar los dispositivos con comodidad, por ejemplo, seleccionando un grupo de administración o una selección de dispositivos.

- Agregar un código de activación o un archivo de clave en los dispositivos manualmente

# Aplicaciones de Kaspersky. Despliegue centralizado

Esta sección describe los métodos para la instalación remota de aplicaciones de Kaspersky y su eliminación desde dispositivos conectados a una red.

Antes de comenzar a desplegar aplicaciones en sus dispositivos cliente, asegúrese de que el hardware y el software de esos dispositivos cliente cumplan con los requisitos aplicables.

El Agente de red es un componente que proporciona la conexión del Servidor de administración con dispositivos cliente. Por lo tanto, se debe instalar en cada dispositivo cliente, que a su vez se debe conectar al sistema de control centralizado remoto. El dispositivo con el Servidor de administración instalado solamente puede usar la versión de servidor del Agente de red. Esta versión se incluye en el Servidor de administración como una parte que se instala y desinstala de forma conjunta. No tiene que instalar el Agente de red en ese dispositivo.

El Agente de red se puede instalar de forma remota o local como cualquier aplicación. Si despliega las aplicaciones de seguridad en forma centralizada a través de la Consola de administración, puede instalar el Agente de red junto con ellas.

Los Agentes de red pueden diferir según las aplicaciones de Kaspersky con las que trabajan. En algunos casos, el Agente de red se puede instalar localmente (para obtener información consulte la documentación para las aplicaciones correspondientes). Solo tiene que instale el Agente de red en un dispositivo cliente una vez.

Las aplicaciones de Kaspersky se administran a través de la Consola de administración usando los complementos de administración. Por lo tanto, para obtener acceso a la interfaz de administración de aplicaciones mediante Kaspersky Security Center, debe instalarse el complemento de administración correspondiente en la estación de trabajo del administrador.

Puede realizar la instalación remota de aplicaciones desde la estación de trabajo del administrador en la ventana principal de Kaspersky Security Center.

Para instalar el software de manera remota, debe crear una tarea de instalación remota.

La tarea creada para la instalación remota se iniciará según su programación. Se puede interrumpir el procedimiento de instalación al detener la tarea de manualmente.

Si la instalación remota de una aplicación arroja un error, asegúrese de que se cumplan los requisitos de preparación del dispositivo.

Puede realizar un seguimiento del progreso de la instalación remota de las aplicaciones de Kaspersky en una red mediante el informe de despliegue.

Para obtener información sobre la administración de las aplicaciones enumeradas en Kaspersky Security Center, consulte la documentación para las aplicaciones correspondientes.

# Reemplazo de aplicaciones de seguridad de terceros

La Instalación de aplicaciones de seguridad de Kaspersky a través de Kaspersky Security Center puede requerir la eliminación del software de terceros incompatible con la aplicación instalada. Kaspersky Security Center proporciona varias formas de eliminar las aplicaciones de terceros.

## Eliminar aplicaciones incompatibles utilizando el instalador

Esta opción está disponible solo en la Consola de administración basada en Microsoft Management Console.

El método del programa de instalación de eliminar aplicaciones incompatibles es compatible con varios tipos de instalación. Antes de la instalación de la aplicación de seguridad, todas las aplicaciones incompatibles se eliminan automáticamente si la ventana de propiedades del paquete de instalación de esta aplicación de seguridad (sección **Aplicaciones incompatibles**) tiene la opción **Desinstalar aplicaciones incompatibles automáticamente** seleccionada.

### Eliminar aplicaciones incompatibles al configurar la instalación remota de una aplicación

Cuando esté configurando la instalación remota de una aplicación de seguridad, puede habilitar la opción **Desinstalar aplicaciones incompatibles automáticamente**. En la Consola de administración basada en Microsoft Management Console (MMC), esta opción está disponible en el Asistente de instalación remota. En Kaspersky Security Center Web Console, puede encontrar esta opción en el Asistente de despliegue de la protección. Cuando esta opción se habilita, Kaspersky Security Center elimina la aplicación incompatible antes de instalar una aplicación de seguridad en un dispositivo administrado.

Instrucciones:

- Consola de administración: Eliminación de aplicaciones mediante el Asistente de instalación remota
- Kaspersky Security Center Web Console: Eliminar aplicaciones incompatibles antes de la instalación

### Eliminar aplicaciones incompatibles a través de una tarea dedicada

Para eliminar aplicaciones incompatibles, use la tarea **Desinstalar aplicación de forma remota**. Esta tarea se debe ejecutar en los dispositivos antes que la tarea para instalar la aplicación de seguridad. Por ejemplo, en la tarea de instalación, puede seleccionar **Al completarse otra tarea** con el tipo de programación, en el que la otra tarea es **Desinstalar aplicación de forma remota**.

Este método de desinstalación es útil cuando el instalador de la aplicación de seguridad no puede eliminar correctamente una aplicación incompatible.

Instrucciones para la Consola de administración: Crear una tarea.

## Instalar aplicaciones mediante la tarea de instalación remota

Kaspersky Security Center permite que usted instale aplicaciones en dispositivos remotamente, usando las tareas de instalación remotas. Las tareas se crean y se asignan a los dispositivos a través de un asistente específico. Para asignar una tarea con mayor facilidad y rapidez, puede especificar los dispositivos (hasta 1000) de distintas maneras a través de la ventana del asistente:

- **Seleccionar dispositivos de la red detectados por el Servidor de administración**. En este caso, la tarea se asigna a dispositivos específicos. Estos pueden ser tanto dispositivos asignados a grupos de administración como dispositivos no asignados.
- **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**. Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

- **Asignar tarea a una selección de dispositivos**. En este caso, la tarea se asigna a los dispositivos incluidos en una selección creada anteriormente. Puede especificar la selección predeterminada o una personalizada que haya creado.

- **Asignar tarea a un grupo de administración**. En este caso, la tarea se asigna a los dispositivos incluidos en el grupo de administración creado anteriormente.

Para evitar problemas que puedan ocurrir durante la instalación de la aplicación en un dispositivo cliente sin Agente de red instalado, debe proceder como se describe en el despliegue forzado a través de la tarea de instalación remota de Kaspersky Security Center.

## Instalar una aplicación en los dispositivos seleccionados

*Instalar una aplicación en los dispositivos seleccionados:*

1. En el árbol de la consola, seleccione la carpeta **Tareas**.

2. Ejecute la creación de la tarea con un clic en el botón **Crear una tarea**.

   Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente.

   En la ventana **Seleccione el tipo de tarea** del Asistente para crear nueva tarea, en el nodo **Servidor de administración de Kaspersky Security Center**, seleccione **Instalar aplicación de forma remota** como tipo de tarea.

   El Asistente para crear nueva tarea crea una tarea de instalación remota para la aplicación seleccionada en dispositivos específicos. La tarea recientemente creada se muestra en el espacio de trabajo de la carpeta **Tareas**.

3. Ejecute la tarea manualmente o espere que se inicie de acuerdo con la programación especificada por usted en la configuración de la tarea.

Al finalizar la tarea de instalación remota, la aplicación seleccionada se instalará en los dispositivos seleccionados.

## Instalar una aplicación en dispositivos cliente del grupo de administración

*Para instalar una aplicación en los dispositivos cliente del grupo de administración:*

1. Establezca conexión con el Servidor de administración que controla el grupo de administración relevante.

2. Seleccione un grupo de administración del árbol de consola.

3. En el espacio de trabajo del grupo, seleccione la pestaña **Tareas**.

4. Ejecute la creación de la tarea con un clic en el botón **Crear una tarea**.

   Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente.

   En la ventana **Seleccione el tipo de tarea** del Asistente para crear nueva tarea, en el nodo **Servidor de administración de Kaspersky Security Center**, seleccione **Instalar aplicación de forma remota** como tipo de tarea.

   El Asistente para crear nueva tarea crea una tarea de grupo de instalación remota para la aplicación seleccionada. La nueva tarea aparece en el espacio de trabajo del grupo de administración en la pestaña **Tareas**.

5. Ejecute la tarea manualmente o espere que se inicie de acuerdo con la programación especificada por usted en la configuración de la tarea.

Al finalizar la tarea de instalación remota, la aplicación seleccionada se instalará en los dispositivos cliente del grupo de administración.

## Instalar una aplicación mediante las directivas de grupo de Active Directory

Si quiere instalar una aplicación de Kaspersky en sus dispositivos administrados a través de Kaspersky Security Center, puede hacerlo mediante directivas de grupo de Active Directory.

Para instalar una aplicación utilizando directivas de grupo de Active Directory, el paquete de instalación de la misma debe incluir el Agente de red.

*Para instalar una aplicación mediante las directivas de grupo de Active Directory:*

1. Ejecute el Asistente de instalación remota para comenzar a configurar la instalación del software.

2. En el Asistente de instalación remota, dentro de la ventana **Definir la configuración de la tarea de instalación remota**, active la opción **Asignar la instalación del paquete en las directivas de grupo de Active Directory**.

3. En la ventana **Seleccionar las cuentas con que se accederá a los dispositivos** del Asistente de instalación remota, seleccione la opción **Se necesita una cuenta (no se utiliza el Agente de red)**.

4. Agregue la cuenta con privilegios de administrador en el dispositivo donde está instalado Kaspersky Security Center o la cuenta incluida en el grupo de dominios Propietarios del creador de directivas de grupo.

5. Asigne los permisos necesarios a la cuenta seleccionada:

    a. Vaya a **Panel de control** → **Herramientas administrativas** y abra **Administración de directivas de grupo**.

    b. Haga clic en el nodo del dominio pertinente.

    c. Haga clic en la sección **Delegación**.

    d. En la lista desplegable **Permiso**, seleccione **Vincular objetos de directiva de grupo**.

    e. Haga clic en **Agregar**.

    f. En la ventana **Seleccionar usuario, equipo o grupo** que se abre, seleccione la cuenta pertinente.

    g. Haga clic en **Aceptar** para cerrar la ventana **Seleccionar usuario, equipo o grupo**.

    h. En la lista **Grupos y usuarios**, seleccione la cuenta que acaba de agregar y, luego, haga clic en **Avanzado** → **Avanzado**.

    i. En la lista **Entradas de permiso**, haga doble clic en la cuenta que acaba de agregar.

    j. Otorgue los siguientes permisos:

    - **Crear objetos de grupo**
    - **Eliminar objetos de grupo**
    - **Crear objetos de contenedor de directivas de grupo**
    - **Eliminar objetos de contenedor de directivas de grupo**

    k. Haga clic en **Aceptar** para guardar los cambios.

6. Siga las instrucciones del asistente para configurar las demás opciones.

7. Ejecute de forma manual la tarea de instalación remota creada o espere a que se inicie según la programación.

Se inicia la siguiente secuencia de instalación remota:

1. Cuando la tarea está en ejecución, en cada dominio que incluya cualquier dispositivo cliente del grupo especificado se crean los siguientes objetos:

    - Un objeto de directiva de grupo (GPO) bajo el nombre **Kaspersky_AK{GUID}**.
    - Un grupo de seguridad que corresponde al GPO. Este grupo de seguridad incluye dispositivos cliente cubiertos por la tarea. El contenido del grupo de seguridad define el alcance del GPO.

2. Kaspersky Security Center instala las aplicaciones de Kaspersky seleccionadas en los dispositivos cliente directamente desde la carpeta KLSHARE (la carpeta compartida en red de la aplicación). En la carpeta de instalación de Kaspersky Security Center, se creará una subcarpeta auxiliar anidada que contendrá el archivo .msi de la aplicación que se instalará.

3. Los dispositivos que sume al alcance de la tarea se agregarán al grupo de seguridad cuando la tarea se ejecute nuevamente. Si la opción **Ejecutar tareas no realizadas** está seleccionada en la programación de tareas, los dispositivos se agregarán de inmediato al grupo de seguridad.

4. Los dispositivos que elimine del alcance de la tarea se quitarán del grupo de seguridad cuando la tarea se ejecute nuevamente.

5. Cuando una tarea se elimina de Active Directory, también se eliminan el GPO, el enlace al GPO y el grupo de seguridad correspondiente.

Si desea aplicar otro esquema de instalación mediante Active Directory, puede configurar los parámetros requeridos manualmente. Por ejemplo, esto puede ser necesario en los siguientes casos:

- Cuando el administrador de la protección antivirus no tiene derechos para hacer cambios en Active Directory de ciertos dominios.
- Cuando el paquete de instalación original debe almacenarse en un recurso de red distinto.
- Cuando resulta necesario vincular un GPO con determinadas unidades de Active Directory.

Existen siguientes opciones para usar un esquema de instalación alternativa a través Active Directory:

- Si la instalación se realizará directamente desde la carpeta compartida de Kaspersky Security Center, en las propiedades del GPO debe especificar el archivo .msi situado en la subcarpeta exec de la carpeta del paquete de instalación para la aplicación requerida.
- Si el paquete de instalación tiene que ubicarse en otro recurso de red, debe copiar en él todo el contenido de la carpeta exec porque, además del archivo con la extensión .msi, la carpeta contiene los archivos de configuración generados cuando se creó el paquete. Para instalar la clave de licencia junto con la aplicación, copie también el archivo de clave a esta carpeta.

## Instalación remota de aplicaciones en dispositivos macOS

*Para instalar aplicaciones en dispositivos que ejecutan macOS mediante una tarea de instalación remota, siga estos pasos:*

1. Cree un archivo que conste de un paquete de instalación y un script de instalación .sh.

2. Deshabilite la opción **Verificar el tipo de sistema operativo antes de la descarga** en el Asistente para crear nueva tarea.

Como alternativa, puede utilizar la tarea **Ejecutar scripts de forma remota**. El siguiente artículo describe cómo configurar archivos para esta tarea: Instalar de forma remota aplicaciones en dispositivos con la tarea Ejecución remota de scripts.

## Instalar aplicaciones en los Servidores de administración secundarios

*Para instalar una aplicación en Servidores de administración secundarios:*

1. Establezca conexión con el Servidor de administración que controla los servidores de administración secundarios pertinentes.

2. Asegúrese de que el paquete de instalación que corresponde a la aplicación que se está instalando esté disponible en cada uno de los Servidores de administración secundarios seleccionados. Si el paquete de instalación no se puede encontrar en ninguno de los Servidores secundarios, distribúyalo usando la tarea de distribución del paquete de instalación.

3. Cree la tarea de instalación de la aplicación en los Servidores de administración secundarios de una de las siguientes maneras:

   - Si desea crear una tarea para los Servidores de administración secundarios en el grupo de administración seleccionado, cree una tarea de grupo de instalación remota para este grupo.
   - Si desea crear una tarea para Servidores de administración secundarios específicos, cree una tarea de instalación remota para dispositivos específicos.

   El Asistente de creación de tareas de despliegue empieza a guiarlo a través de la creación de la tarea de instalación remota. Siga las instrucciones del asistente.

   En la ventana **Seleccione el tipo de tarea** del Asistente para crear nueva tarea, en la sección **Servidor de administración de Kaspersky Security Center**, abra la carpeta **Avanzado** y seleccione la tarea **Instalar aplicación en Servidores de administración secundarios de forma remota** como el tipo de tarea.

   El Asistente para crear nueva tarea creará la tarea de instalación remota de la aplicación seleccionada en los Servidores de administración secundarios específicos.

4. Ejecute la tarea manualmente o espere que se inicie de acuerdo con la programación especificada por usted en la configuración de la tarea.

Al finalizar la tarea de instalación remota, la aplicación seleccionada se instalará en los Servidores de administración secundarios.

# Instalar aplicaciones mediante el Asistente de instalación remota

Para instalar las aplicaciones de Kaspersky, se puede usar el Asistente de instalación remota. El Asistente de instalación remota permite la instalación remota de las aplicaciones a través de paquetes de instalación creados especialmente o de manera directa desde un paquete de distribución.

Para el buen funcionamiento de la tarea de instalación remota en un dispositivo cliente en el cual no se ha instalado ningún Agente de red, se deben abrir los siguientes puertos: TCP 139 y 445; UDP 137 y 138. De manera predeterminada, estos puertos se abren para todos los dispositivos incluidos en el dominio. En caso de errores de red, consulte la Base de conocimientos de Kaspersky Security Center.

*Para instalar la aplicación en los dispositivos seleccionados usando el Asistente de instalación remota:*

1. En el árbol de consola, busque la carpeta **Instalación remota** y seleccione la subcarpeta **Paquetes de instalación**.
2. En el espacio de trabajo de la carpeta, seleccione el paquete de instalación de la aplicación que debe instalar.
3. En el menú contextual del paquete de instalación, seleccione **Instalar aplicación**.

   Se inicia el Asistente de instalación remota.

4. En la ventana **Seleccionar los dispositivos para la instalación**, puede crear una lista de los dispositivos en los cuales la aplicación será instalada:

   - **Instalar en un grupo de dispositivos administrados**

     Si selecciona esta opción, la tarea de instalación remota se creará para un grupo de dispositivos.

   - **Seleccionar los dispositivos para la instalación**

     Si se selecciona esta opción, se crea la tarea de instalación remota para dispositivos específicos. Esos dispositivos específicos pueden incluir tanto dispositivos administrados como no asignados.

5. En la ventana **Definir la configuración de la tarea de instalación remota**, especifique la configuración para la instalación remota de la aplicación.

   En el grupo de configuraciones **Forzar la descarga del paquete de instalación**, puede especificar cómo se distribuyen a los dispositivos cliente los archivos que se requieren para la instalación de una aplicación:

   - **Con el Agente de red**

     Si habilita esta opción, los paquetes de instalación se transferirán a los dispositivos cliente a través del Agente de red instalado en esos dispositivos.

     Si no habilita esta opción, los paquetes de instalación se distribuirán utilizando las herramientas provistas por el sistema operativo de los dispositivos cliente.

     Recomendamos habilitar esta opción si la tarea está asignada a dispositivos que tienen instalado el Agente de red.

     Esta opción está habilitada de manera predeterminada.

   - **Con los recursos del sistema operativo a través del Servidor de administración**

     Si se habilita esta opción, los archivos se transmitirán a los dispositivos cliente a través del Servidor de administración utilizando las herramientas provistas por el sistema operativo de los dispositivos cliente. Puede habilitar esta opción si no hay ningún Agente de red instalado en el dispositivo cliente, pero el dispositivo cliente está en la misma red que el Servidor de administración.

     Esta opción está activada de forma predeterminada.

   - **Con los recursos del sistema operativo a través de los puntos de distribución**

     Si habilita esta opción, los paquetes de instalación se transferirán a los dispositivos cliente mediante las herramientas del sistema operativo a través de los puntos de distribución. Puede seleccionar esta opción si existe al menos un punto de distribución en la red.

     Si habilitó la opción **Con el Agente de red**, las herramientas del sistema operativo se utilizarán para transferir los archivos solo si las herramientas del Agente de red no están disponibles.

     Está opción se habilita de manera predeterminada para las tareas de instalación remota creadas en servidores de administración virtuales.

   - **Número de intentos de instalación**

Si, al ejecutar la tarea de instalación remota, Kaspersky Security Center no puede instalar una aplicación en un dispositivo administrado dentro del número de ejecuciones del instalador especificadas por el parámetro, Kaspersky Security Center deja de entregar el paquete de instalación a este dispositivo administrado y ya no inicia el instalador en el dispositivo.

La opción `Número de intentos de instalación` permite que guarde los recursos del dispositivo administrado, así como reducir el tráfico (desinstalación, ejecución de archivos MSI y mensajes de error).

Los intentos de inicio de tareas recurrentes pueden indicar un problema en el dispositivo que impide la instalación. El administrador debe resolver el problema dentro del número especificado de intentos de instalación (por ejemplo, asignando suficiente espacio en el disco, eliminando aplicaciones incompatibles o modificando la configuración de otras aplicaciones que impidan la instalación) y para reiniciar la tarea (manualmente o de manera programada).

Si finalmente no se logra la instalación, el problema se considera no resuelto y cualquier inicio de tarea adicional se considera costoso en términos de consumo innecesario de recursos y tráfico.

Cuando se crea la tarea, el contador de intentos se establece en `0`. Cada ejecución del instalador que devuelve un error en el dispositivo incrementa la lectura del contador.

Si se superó la cantidad de intentos especificada en el parámetro y el dispositivo está listo para la instalación de la aplicación, puede aumentar el valor del parámetro `Cantidad de intentos de instalación` e iniciar la tarea para instalar la aplicación. Alternativamente, puede crear una nueva tarea de instalación remota.

Defina qué hacer con los dispositivos cliente administrados por otro Servidor de administración:

- **Instalar en todos los dispositivos**

  La aplicación se instalará incluso en dispositivos administrados por otros Servidores de administración.

  Esta opción está seleccionada de manera predeterminada. Si solo tiene un Servidor de administración en la red, no es necesario que cambie esta opción.

- **Instalar solo en dispositivos administrados a través de este Servidor de administración**

  La aplicación se instalará solo en los dispositivos administrados por este Servidor de administración. Seleccione esta opción si tiene más de un Servidor de administración en su red y desea evitar conflictos entre ellos.

Configure las opciones adicionales:

- **No reinstalar la aplicación si ya está instalada**

  Si habilita esta opción y se detecta que la aplicación ya está instalada en el dispositivo cliente, no se la reinstalará.

  Si no habilita esta opción, la aplicación se instalará en todos los casos.

  Esta opción está activada de forma predeterminada.

- **Asignar la instalación del paquete en las directivas de grupo de Active Directory**

Si se habilita esta opción, se instala un paquete de instalación mediante las directivas de grupo de Active Directory.

Esta opción se encuentra disponible si se selecciona el paquete de instalación del Agente de red.

Esta opción está deshabilitada de forma predeterminada.

6. En la ventana **Seleccionar una clave de licencia**, seleccione una clave de licencia y un método de distribución:

- **No incluir la clave de licencia o código de activación en el paquete de instalación (recomendado)**

  La clave se distribuirá automáticamente a todos los dispositivos con los que sea compatible si se cumplen las siguientes condiciones:

  - Si se habilitó la distribución automática en las propiedades de la clave.
  - Si se creó la tarea **Agregar clave**.

- **Incluir la clave de licencia en el paquete de instalación**

  La clave se distribuirá a los dispositivos con el paquete de instalación.

  No le recomendamos distribuir la clave con este método, ya que los derechos Acceso de lectura compartidos están activados para el repositorio de paquetes de instalación.

La ventana **Seleccionar una clave de licencia** se muestra si el paquete de instalación no contiene una clave de licencia.

Si el paquete de instalación incluye una clave de licencia, se muestra la ventana **Propiedades de la clave de licencia**, que contiene los detalles de la clave de licencia.

7. En la ventana **Seleccione la opción de reinicio del sistema operativo**, especifique si los dispositivos se deben reiniciar si el sistema operativo se debe reiniciar durante la instalación de aplicaciones en ellos:

- **No reiniciar el dispositivo**

  Si se selecciona esta opción, el dispositivo no se reiniciará después de instalar la aplicación de seguridad.

- **Reiniciar el dispositivo**

  Si se selecciona esta opción, el dispositivo se reiniciará después de instalar la aplicación de seguridad.

- **Solicitar al usuario una acción**

  Si se selecciona esta opción, después de instalar la aplicación de seguridad se mostrará una notificación al usuario donde se informa que es necesario reiniciar el dispositivo. Mediante el vínculo **Modificar**, puede modificar el texto del mensaje, la duración del mensaje y el momento de reinicio automático.

  Esta opción está seleccionada de forma predeterminada.

- **Forzar el cierre de aplicaciones en sesiones bloqueadas**

  Si se habilita esta opción, se forzará el cierre de las aplicaciones de un dispositivo bloqueado antes de que se reinicie el dispositivo.

  Esta opción está deshabilitada de forma predeterminada.

8. En la ventana **Seleccione las cuentas con que se accederá a los dispositivos**, puede agregar las cuentas que se usarán para iniciar la tarea de instalación remota:

   - **No se necesita una cuenta (el Agente de red está instalado)**

     Si selecciona esta opción, no necesitará especificar la cuenta con la que se ejecutará el instalador de la aplicación. Para ejecutar la tarea, se usará la cuenta con la que se haya iniciado el servicio del Servidor de administración.

     Esta opción no está disponible si el Agente de red no se instaló en los dispositivos cliente.

   - **Se necesita una cuenta (no se utiliza el Agente de red)**

     Seleccione esta opción si el Agente de red no está instalado en los dispositivos a los que asigna la tarea de instalación remota. En este caso, puede especificar una cuenta de usuario o un certificado SSH para instalar la aplicación.

     - **Cuenta local**. Si se selecciona esta opción, especifique la cuenta bajo la que se ejecutará el instalador de aplicación. Haga clic en el botón **Agregar**, seleccione **Cuenta local** y, a continuación, especifique las credenciales de la cuenta de usuario.

       Puede especificar varias cuentas de usuario si, por ejemplo, ninguna de ellas tiene todos los derechos requeridos en todos los dispositivos a los que asigne esta tarea. En este caso, todas las cuentas añadidas se utilizan para ejecutar la tarea, en orden consecutivo de arriba abajo.

     - **Certificado de SSH**. Si desea instalar una aplicación en un dispositivo cliente basado en Linux, puede especificar un certificado SSH en lugar de una cuenta de usuario. Haga clic en el botón **Agregar**, seleccione **Certificado de SSH** y, a continuación, especifique las claves pública y privada del certificado.

       Para generar una clave privada, puede utilizar la utilidad ssh-keygen. Tenga en cuenta que Kaspersky Security Center espera que la clave privada esté en formato PEM, pero, de manera predeterminada, la utilidad ssh-keygen genera claves SSH en formato OPENSSH. Kaspersky Security Center no admite el formato OPENSSH. Para crear una clave privada en el formato PEM admitido, agregue la opción -m PEM en el comando ssh-keygen. Por ejemplo:

       ```
       ssh-keygen -m PEM -t rsa -b 4096 -C "<correo electrónico del usuario>"
       ```

9. En la ventana **Inicio de la instalación**, haga clic en el botón **Siguiente** para crear e iniciar una tarea de instalación remota en los dispositivos seleccionados.

   Si la ventana **Inicio de la instalación** tiene la opción **No ejecutar la tarea después de que el Asistente de instalación remota finalice** seleccionada, la tarea de instalación remota no se iniciará. Podrá iniciar esta tarea de manera manual en otro momento. El nombre de la tarea equivale al nombre del paquete de instalación para la aplicación: **Instalación de <nombre del paquete de instalación>**.

*Para instalar la aplicación en los dispositivos seleccionados en un grupo de administración usando el Asistente de instalación remota, realice lo siguiente:*

1. Establezca conexión con el Servidor de administración que controla el grupo de administración relevante.

2. Seleccione un grupo de administración del árbol de consola.

3. En el espacio de trabajo del grupo, haga clic en el botón **Realizar acción** y seleccione **Instalar aplicación** en la lista desplegable.

   Esto iniciará el Asistente de instalación remota. Siga las instrucciones del asistente.

4. En el paso final del asistente, haga clic en **Siguiente** para crear y ejecutar una tarea de instalación remota en los dispositivos seleccionados.

Cuando se completa el Asistente de instalación remota, Kaspersky Security Center realiza las siguientes acciones:

- Crea el paquete de instalación para la instalación de la aplicación (si no se creó anteriormente). El paquete de instalación estará ubicado en la carpeta **Instalación remota**, en la subcarpeta **Paquetes de instalación**, con un nombre que corresponda al nombre y la versión de la aplicación. El paquete puede usarse para instalar la aplicación en otro momento.

- Crea y ejecuta una tarea de instalación remota para dispositivos específicos o para un grupo de administración. La tarea de instalación remota creada recientemente se almacena en la carpeta **Tareas** o se agrega a las tareas del grupo de administración para el cual se creó. Podrá iniciar esta tarea de manera manual en otro momento. El nombre de la tarea equivale al nombre del paquete de instalación para la aplicación: **Instalación de <nombre del paquete de instalación>**.

# Trabajar con los complementos de administración

Las aplicaciones de Kaspersky se administran a través de la Consola de administración usando los complementos de administración. Cada aplicación de Kaspersky que se puede administrar a través de Kaspersky Security Center incluye un complemento de administración. Mediante el complemento de administración de aplicaciones, es posible realizar las siguientes acciones en la Consola de administración:

- Crear y editar las directivas y la configuración de la aplicación, además de la configuración de las tareas de la aplicación.

- Obtener información sobre las tareas, los eventos y las estadísticas de funcionamiento de la aplicación que se recibieron desde dispositivos cliente.

*Para revisar la lista de complementos instalados y sus versiones:*

1. En el árbol de la Consola de administración, haga clic con el botón derecho en **Servidor de administración <Nombre_de_servidor>** y seleccione **Propiedades**.

2. Haga clic en **Avanzado** → **Detalles de los complementos de administración de aplicaciones instalados**.

La lista de complementos de administración instalados y sus versiones aparece en el panel derecho.

Puede instalar los complementos de las aplicaciones administradas cuando ejecuta el asistente de inicio rápido del Servidor de administración durante la configuración inicial de Kaspersky Security Center. Además, puede instalar los complementos de administración de forma manual.

*Para instalar un complemento de administración manualmente:*

1. Descargue el complemento de administración para la aplicación de Kaspersky y la versión requerida (por ejemplo, Kaspersky Endpoint Security para Windows 12.6) desde la página web del Servicio de soporte técnico de Kaspersky.

2. Si la Consola de administración se está ejecutando, ciérrela.

3. Descomprima el archivo del complemento descargado y ejecute el archivo klcfginst.msi o klcfginst.exe. Siga las instrucciones del asistente de instalación.

4. Cuando se complete la instalación, ejecute la Consola de administración y asegúrese de que el complemento aparezca en la lista de complementos instalados, como se describe en el procedimiento anterior.

Cuando ejecuta la Consola de administración después de instalar un complemento de administración que admite el Asistente de inicio rápido de aplicaciones administradas, el asistente se inicia automáticamente. Puede seguir los pasos del Asistente de inicio rápido de aplicaciones administradas para crear directivas y tareas predeterminadas de la aplicación de Kaspersky. El asistente se inicia automáticamente solo cuando ejecuta la Consola de administración después de la primera instalación del complemento o después de actualizar el complemento de administración a una versión que sea compatible con otra versión de la aplicación de Kaspersky para la cual aún no se crearon tareas ni directivas. También puede iniciar el Asistente de inicio rápido de aplicaciones administradas de forma manual.

*Para iniciar el Asistente de inicio rápido de aplicaciones administradas manualmente:*

1. En el árbol de consola, haga clic el nodo del **Servidor de administración**.

2. En el menú contextual del nodo Servidor de administración, seleccione **Todas las tareas → Asistente de inicio rápido de aplicaciones administradas**.

3. Se inicia el Asistente de inicio rápido de aplicaciones administradas. Siga los pasos del asistente para crear directivas y tareas predeterminadas de la aplicación de Kaspersky.

*Para eliminar un complemento de administración:*

1. Si la Consola de administración se está ejecutando, ciérrela.

2. Abra el Editor del Registro de Windows.

3. Busque la siguiente clave:

   - `HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\28\Plugins` para un sistema de 32 bits.

   - `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins` para un sistema de 64 bits.

   La clave contiene los complementos de administración instalados. Para cada complemento, el valor de `DisplayName` contiene el nombre del complemento y el valor de `UninstallString` contiene el comando para desinstalar el complemento.

4. Busque la clave del complemento que desee desinstalar y copie el valor de `UninstallString` al portapapeles.

5. Pegue el valor en la cadena de comandos y ejecútelo con derechos de administrador del sistema.

La versión del complemento de administración no debe ser anterior a la versión de la aplicación administrada de Kaspersky. Si actualiza la aplicación de Kaspersky en los dispositivos, debe instalar el complemento de administración de la misma versión.

Cuando abra la directiva que se creó en una versión anterior del complemento, se le solicitará que acepte la Declaración de Kaspersky Security Network.

Si desinstala Kaspersky Security Center Web Console, también se desinstalan todos los complementos de administración.

Si abre y guarda la directiva en la versión del complemento posterior a la versión de la aplicación administrada, la directiva se actualizará y no podrá abrirla en el complemento de la versión anterior.

# Ver un informe sobre el despliegue de la protección

Puede usar el informe del despliegue de la protección para controlar cómo progresa el despliegue de la protección en la red.

*Para ver un informe sobre el despliegue de la protección:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.

2. En el espacio de trabajo del nodo, abra la pestaña **Informes**.

3. En el espacio de trabajo de la carpeta **Informes**, seleccione la plantilla de informe denominada **Informe del despliegue de la protección**.

El espacio de trabajo muestra un informe que contiene información sobre el despliegue de la protección en todos los dispositivos conectados a la red.

Puede generar un nuevo informe sobre el despliegue de la protección y especificar el tipo de datos que debe incluir:

- Para un grupo de administración

- Para dispositivos específicos

- Para una selección de dispositivos
- Para todos los dispositivos

Kaspersky Security Center supone que la protección se distribuye en un dispositivo si una aplicación de seguridad se instala y la protección en tiempo real se habilita.

# Eliminar aplicaciones de manera remota

Kaspersky Security Center le permite desinstalar aplicaciones de dispositivos de manera remota a través de tareas de la desinstalación remotas. Las tareas se crean y se asignan a los dispositivos a través de un asistente específico. Para designar los dispositivos de la tarea con mayor facilidad y rapidez, puede seleccionarlos de distintas maneras a través de la ventana del asistente:

- **Seleccionar dispositivos de la red detectados por el Servidor de administración**. En este caso, la tarea se asigna a dispositivos específicos. Estos pueden ser tanto dispositivos asignados a grupos de administración como dispositivos no asignados.
- **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**. Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.
- **Asignar tarea a una selección de dispositivos**. En este caso, la tarea se asigna a los dispositivos incluidos en una selección creada anteriormente. Puede especificar la selección predeterminada o una personalizada que haya creado.
- **Asignar tarea a un grupo de administración**. En este caso, la tarea se asigna a los dispositivos incluidos en el grupo de administración creado anteriormente.

## Problemas con la eliminación remota

Al realizar la eliminación remota de aplicaciones de terceros, los administradores pueden encontrar una advertencia que pone: "La desinstalación remota ha finalizado en este dispositivo con advertencias: la aplicación que se quería eliminar no está instalada". Este problema suele surgir cuando la aplicación que se quiere a eliminar está instalada solo para el usuario individual que está conectado actualmente. Si el usuario no ha iniciado sesión, dicha aplicación se vuelve invisible y no puede eliminarse de forma remota.

Este comportamiento difiere del de las aplicaciones diseñadas para ser utilizadas por múltiples usuarios en el mismo dispositivo, donde las aplicaciones son visibles y accesibles globalmente para todos los usuarios del dispositivo.

Dentro de Kaspersky Security Center, el algoritmo de registro de aplicaciones gestiona de manera diferente las aplicaciones para usuarios individuales y las aplicaciones para múltiples usuarios:

- Las aplicaciones para múltiples usuarios se mantienen en una lista actualizada y en tiempo real de aplicaciones instaladas por el instalador.
- Las aplicaciones de usuarios individuales se monitorean mediante un mecanismo de almacenamiento en caché.

  Si un usuario ha iniciado sesión en el momento de la detección de la aplicación, Kaspersky Security Center almacena en caché información sobre las aplicaciones de ese usuario. Incluso si el usuario cierra sesión más tarde, Kaspersky Security Center continúa mostrando estas aplicaciones como instaladas según los datos almacenados en caché, aunque ya no estén visibles ni accesibles en el dispositivo.

Esta discrepancia puede generar situaciones en las que Kaspersky Security Center identifica una aplicación como instalada basándose en datos almacenados en caché, pero la tarea de eliminación de la aplicación falla porque la aplicación no es accesible cuando el usuario cierra la sesión.

De forma predeterminada, la vida útil de los datos de la aplicación almacenados en caché se establece en 30 días. Los administradores pueden modificar este ajuste para reducir la duración de la memoria caché, minimizando así las discrepancias entre los datos que se muestran y la visibilidad real de la aplicación en los dispositivos.

Para ajustar la duración de la memoria caché a 1 hora (3600 segundos), ejecute el siguiente comando en el Servidor de administración:

```
klscflag -fset -pv klserver -n KLNAG_INV_PERUSER_APPS_CACHE_NONACTIVE_SIDS_LIFETIME_SEC
-t d -v 3600
```

Después de ejecutar este comando, reinicie el Servidor de administración para que los cambios surtan efecto.

## Orígenes de la información acerca de aplicaciones instaladas

El Agente de red recupera de las siguientes claves de registro información sobre el software instalado en los dispositivos Windows:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

  Contiene información sobre las aplicaciones instaladas para todos los usuarios.
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

  Contiene información sobre las aplicaciones instaladas para todos los usuarios.
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

  Contiene información sobre las aplicaciones que el usuario actual tiene instaladas.
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

  Contiene información sobre las aplicaciones instaladas para usuarios específicos.

## Eliminación remota de una aplicación de dispositivos cliente del grupo de administración

*Para eliminar de manera remota una aplicación de dispositivos cliente de un grupo de administración:*

1. Establezca conexión con el Servidor de administración que controla el grupo de administración relevante.
2. Seleccione un grupo de administración del árbol de consola.
3. En el espacio de trabajo del grupo, seleccione la pestaña **Tareas**.
4. Ejecute la creación de la tarea con un clic en el botón **Nueva tarea**.

   Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente.

   En la ventana **Seleccione el tipo de tarea** del Asistente para crear nueva tarea, en el nodo **Servidor de administración de Kaspersky Security Center**, en la carpeta **Avanzado**, seleccione la tarea **Desinstalar aplicación de forma remota**.

   El Asistente para crear nueva tarea crea una tarea de grupo de eliminación remota para la aplicación seleccionada. La nueva tarea aparece en el espacio de trabajo del grupo de administración en la pestaña **Tareas**.
5. Ejecute la tarea manualmente o espere que se inicie de acuerdo con la programación especificada por usted en la configuración de la tarea.

Al finalizar la tarea de instalación remota, la aplicación seleccionada se eliminará de los dispositivos cliente del grupo de administración.

## Eliminación remota de una aplicación de dispositivos seleccionados

*Para eliminar de manera remota una aplicación de dispositivos seleccionados:*

1. En el árbol de la consola, seleccione la carpeta **Tareas**.
2. Ejecute la creación de tareas haciendo clic en **Nueva tarea**.

   Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente.

   En la ventana **Seleccione el tipo de tarea** del Asistente para crear nueva tarea, en el nodo **Servidor de administración de Kaspersky Security Center**, en la carpeta **Avanzado**, seleccione la tarea **Desinstalar aplicación de forma remota**.

   El Asistente para crear nueva tarea crea una tarea de eliminación remota de la aplicación seleccionada en los dispositivos específicos. La tarea recientemente creada se muestra en el espacio de trabajo de la carpeta **Tareas**.
3. Ejecute la tarea manualmente o espere que se inicie de acuerdo con la programación especificada por usted en la configuración de la tarea.

Al finalizar la tarea de eliminación remota, la aplicación seleccionada se eliminará de los dispositivos seleccionados.

# Trabajar con paquetes de instalación

Al crear las tareas de instalación remota, el sistema usa los paquetes de instalación que contienen los conjuntos de parámetros necesarios para la instalación de software.

Los paquetes de instalación pueden contener un archivo de clave. Recomendamos que evite compartir el acceso a los paquetes de instalación que contengan un archivo de clave.

Puede usar un único paquete de instalación varias veces.

Los paquetes de instalación creados para el Servidor de administración se mueven al árbol de consola y se ubican en la carpeta **Instalación remota**, en la subcarpeta **Paquetes de instalación**. Los paquetes de instalación se almacenan en el Servidor de administración en la subcarpeta de servicios de paquete en la carpeta compartida especificada.

Si es necesario, puede eliminar un paquete de instalación de la subcarpeta **Paquetes de instalación** mediante las instrucciones del artículo Eliminación de un objeto.

No cambie el contenido de los paquetes de instalación en una carpeta compartida manualmente. Si es necesario, puede crear una copia de un paquete de instalación, realizar los cambios necesarios y crear nuevas tareas de instalación.

## Creación del paquete de instalación

En este artículo, se describe el procedimiento para crear los siguientes tipos de paquetes de instalación:

- Paquete de instalación para una aplicación de Kaspersky
- Paquete de instalación para un archivo ejecutable específico
- Paquete de instalación para una aplicación de la base de datos de Kaspersky

No hay necesidad de crear manualmente un paquete de instalación para la instalación remota del Agente de red. Se crea de manera automática durante la instalación de Kaspersky Security Center y se guarda en la carpeta **Paquetes de instalación**. Si se eliminó el paquete para la instalación remota del Agente de red, puede volver a crearlo: seleccione el archivo nagent.kud en la carpeta NetAgent del paquete de distribución de Kaspersky Security Center.

*Pasos para crear un paquete de instalación:*

1. Conéctese al Servidor de administración necesario.
2. En el árbol de la consola, vaya a **Avanzado** → **Instalación remota** → **Paquetes de instalación**.

3. Siga uno de estos pasos para comenzar a crear un nuevo paquete de instalación:

   - Haga clic derecho en la carpeta **Paquetes de instalación** y luego seleccione **Nuevo → Paquete de instalación** en el menú contextual.
   - Haga clic derecho en el área vacía de la lista de paquetes de instalación y luego seleccione **Crear → Paquete de instalación** en el menú contextual.
   - Haga clic en **Crear paquete de instalación** en la sección de administración de la lista de paquetes de instalación.

   Se inicia el Asistente de nuevo paquete.

4. Haga clic en el ícono correspondiente para seleccionar uno de los siguientes tipos de paquetes de instalación:

   - Paquete de instalación para una aplicación de Kaspersky.
   - Paquete de instalación para un archivo ejecutable especificado.
   - Paquete de instalación para una aplicación de la base de datos de Kaspersky.

5. Indique el nombre del paquete de instalación que se creará.

   Puede usar cualquier nombre.

6. Use uno de los siguientes métodos para seleccionar la aplicación o el archivo ejecutable relacionado con el paquete de instalación que se creará:

   - Haga clic en el botón **Examinar** y, en la ventana **Abrir** convencional de Windows, seleccione el paquete de distribución de la aplicación requerida que se encuentra en los discos disponibles.

     Esta opción es pertinente si decide crear un paquete de instalación para una aplicación de Kaspersky o para un archivo ejecutable especificado.

   - Haga clic en el botón **Examinar** y, en la ventana **Seleccionar aplicación**, seleccione el paquete de distribución de la aplicación requerida.

     Esta opción es pertinente si decide crear un paquete de instalación para una aplicación de la base de datos de Kaspersky.

   Si necesita crear un paquete de instalación para el Servidor de administración, seleccione el archivo sc.kud. El archivo sc.kud se encuentra en la carpeta raíz del paquete de distribución de Kaspersky Security Center.

   No especifique ningún detalle de cuentas privilegiadas en los parámetros de los paquetes de instalación.

7. Revise el Contrato de licencia de usuario final y la Política de privacidad.

   Cuando cree un paquete de instalación para una aplicación, es posible que se le solicite ver y aceptar un Contrato de licencia de usuario final y una Política de privacidad de la aplicación.

   Lea ambos documentos. Si está de acuerdo con todas las condiciones del Contrato de licencia y de la Política de privacidad, marque las casillas correspondientes.

   Continuará la instalación de la aplicación en su dispositivo y se reanudará la creación del paquete de instalación.

   Si crea un paquete de instalación para Kaspersky Endpoint Security for Mac, puede seleccionar el idioma del Contrato de licencia y de la Política de privacidad.

8. Si es necesario, habilite la instalación automática de los componentes del sistema.

   Si crea un paquete de instalación para una aplicación de la base de datos de Kaspersky, puede habilitar la instalación automática de los componentes del sistema necesarios. El Asistente de nuevo paquete muestra una lista de todos los componentes del sistema disponibles para la aplicación seleccionada. Puede acceder a esta lista en cualquier momento en las propiedades del paquete de instalación.

   Si crea un paquete de instalación para un parche, la lista incluye todos los componentes del sistema necesarios para su despliegue.

9. Haga clic en el botón **Finalizar** para completar el proceso de creación del paquete.

Cuando finalice el Asistente de nuevo paquete, el nuevo paquete de instalación aparecerá en el espacio de trabajo de la carpeta **Paquetes de instalación**, en el árbol de la consola.

## Creación de paquetes de instalación independientes

Usted y los usuarios de dispositivos de su organización pueden utilizar paquetes de instalación independientes para instalar aplicaciones en dispositivos de forma manual.

Un paquete de instalación independiente es un archivo ejecutable (installer.exe) que puede almacenar en el Servidor web o en una carpeta compartida, o transferir al dispositivo cliente mediante algún otro método. También puede enviar un enlace al paquete de instalación independiente por correo electrónico. En el dispositivo cliente, el usuario puede ejecutar el archivo recibido localmente para instalar una aplicación sin utilizar Kaspersky Security Center.

Asegúrese de que el paquete de instalación independiente no esté disponible para personas no autorizadas.

Puede crear paquetes de instalación independientes de aplicaciones de Kaspersky y de aplicaciones de terceros para plataformas Windows, macOS y Linux. Para crear un paquete de instalación independiente para una aplicación de terceros, debe crear un paquete de instalación personalizada.

La fuente para crear paquetes de instalación independientes son los paquetes de instalación en la lista de creados en el Servidor de administración.

*Para crear un paquete de instalación independiente:*

1. En el árbol de consola, haga clic en **Servidor de administración → Avanzado → Instalación remota → Paquetes de instalación**.

   Se muestra una lista de paquetes de instalación disponibles en el Servidor de administración.

2. En la lista de paquetes de instalación, seleccione un paquete de instalación para el que desee crear un paquete independiente.

3. En el menú contextual, seleccione **Crear un paquete de instalación independiente**.

   Se inicia el asistente de creación de paquetes de instalación independiente. Avance por el asistente utilizando el botón **Siguiente**.

4. En la primera página del asistente, si ha seleccionado un paquete de instalación para la aplicación Kaspersky y desea instalar el Agente de red junto con la aplicación seleccionada, verifique de que la opción **Instalar el Agente de red junto con esta aplicación** está habilitada.

   Esta opción está activada de forma predeterminada. Recomendamos que active esta opción si no sabe si el Agente de red está instalado en el dispositivo. Si el Agente de red ya está instalado en el dispositivo, una vez que instale el paquete de instalación independiente con el Agente de red, este último se actualizará a la versión más reciente.

   Si deshabilita esta opción, el Agente de red no se instalará en el dispositivo, y el dispositivo quedará como dispositivo no administrado.

   El asistente le indicará si el Servidor de administración ya cuenta con un paquete de instalación independiente para la aplicación seleccionada. Si esto sucede, elija una de estas acciones:

   - **Crear un paquete de instalación independiente**. Seleccione esta opción si, por ejemplo, desea crear un paquete de instalación independiente para una nueva versión de la aplicación y también conservar un paquete de instalación independiente que haya creado para una versión de la aplicación anterior. El nuevo paquete de instalación independiente se ubicará en otra carpeta.

   - **Utilizar un paquete de instalación independiente que ya existe**. Seleccione esta opción si desea utilizar un paquete de instalación independiente que ya exista. El proceso para crear paquetes no se iniciará.

   - **Volver a generar un paquete de instalación independiente que ya existe**. Seleccione esta opción si desea volver a crear un paquete de instalación independiente para la misma aplicación. El paquete de instalación independiente se ubicará en la misma carpeta.

5. En la siguiente página del asistente, seleccione la opción **Mover los dispositivos no asignados a este grupo** y especifique un grupo de administración al que desea mover el dispositivo cliente después de la instalación del Agente de red.

   De forma predeterminada, el dispositivo se moverá al grupo **Dispositivos administrados**.

   Si no desea mover el dispositivo cliente a ningún grupo de administración después de la instalación del Agente de red, seleccione la opción **No mover los dispositivos**.

6. En la página siguiente del asistente, cuando finaliza el proceso de creación del paquete de instalación independiente, se muestra el resultado de la creación del paquete independiente y una ruta al paquete independiente.

   Puede hacer clic en los enlaces y hacer lo siguiente:

   - Abra la carpeta con el paquete de instalación independiente.

   - Enviar el enlace al paquete de instalación independiente creado por correo electrónico. Para realizar esta acción, debe tener una aplicación de correo electrónico iniciada.

   - Ejemplo de código HTML para la publicación del enlace en un sitio web. Se crea y abre un archivo TXT en una aplicación que está asociada con un formato TXT. En el archivo, se muestra la etiqueta HTML <a> con atributos.

7. En la siguiente página del asistente, si desea abrir la lista de paquetes de instalación independientes, active la opción **Abrir la lista de paquetes independientes**.

8. Haga clic en el botón **FINALIZAR**.

   El Asistente de creación de un paquete de instalación independiente se cierra.

Se crea el paquete de instalación independiente y se lo ubica en la subcarpeta PkgInst de la carpeta compartida del Servidor de administración. Puede ver la lista de paquetes independientes si hace clic en el botón **Ver la lista de paquetes independientes** que se encuentra arriba de la lista de paquetes de instalación.

# Crear un paquete de instalación personalizado

Puede utilizar paquetes de instalación personalizada para hacer lo siguiente:

- Para instalar cualquier aplicación (como un editor de texto) en un dispositivo cliente, por ejemplo, mediante una tarea.
- para crear un paquete de instalación independiente.

Un paquete de instalación personalizada es una carpeta con un conjunto de archivos. La fuente para crear un paquete de instalación personalizada es un *archivo de almacenamiento*. El archivo de almacenamiento contiene un archivo o archivos que deben incluirse en el paquete de instalación personalizada. Al crear un paquete de instalación personalizada, puede especificar parámetros de línea de comandos, por ejemplo, para instalar la aplicación en modo silencioso.

*Para crear un paquete de instalación personalizado:*

1. En el árbol de la consola, seleccione el **Servidor de administración** → **Avanzado** → **Instalación remota** → **Paquetes de instalación**.

   Se muestra una lista de paquetes de instalación disponibles en el Servidor de administración.

2. Encima de la lista de paquetes de instalación, haga clic en el botón **Crear paquete de instalación**.

   Se inicia el Asistente de nuevo paquete. Avance por el asistente utilizando el botón **Next**.

3. En la primera página del Asistente, seleccione **Crear un paquete de instalación para el archivo ejecutable especificado**.

4. En la siguiente página del asistente, especifique el nombre del paquete de instalación personalizada.

5. En la siguiente página del asistente, haga clic en el botón **Examinar** y, en una ventana estándar de Windows **Abrir**, elija un archivo de almacenamiento ubicado en los discos disponibles para crear un paquete de instalación personalizada.

   Puede cargar un archivo comprimido ZIP, CAB, TAR o TAR.GZ. No es posible crear un paquete de instalación a partir de un archivo autoextraíble SFX.

   Los archivos se descargan al Servidor de administración de Kaspersky Security Center.

6. En la siguiente página del asistente, especifique los parámetros de la línea de comandos de un archivo ejecutable.

   Puede especificar parámetros de línea de comandos para instalar la aplicación desde el paquete de instalación en modo silencioso. La especificación de los parámetros de la línea de comandos es opcional.

   Si lo desea, configure las siguientes opciones:

   - **Copiar toda la carpeta al paquete de instalación**

     Seleccione esta opción si el archivo ejecutable está acompañado de otros que también se requieren para instalar la aplicación. Antes de habilitar esta opción, asegúrese de que todos los archivos pertinentes estén almacenados en la misma carpeta. Si habilita esta opción, la aplicación agregará todo el contenido de la carpeta, incluido el archivo ejecutable especificado, al paquete de instalación.

   - **Convertir valores de configuración a los recomendados para las aplicaciones que Kaspersky Security Center reconoce**

     Si la base de datos de Kaspersky contiene la información pertinente, la aplicación se instalará con los parámetros recomendados.

     Dichos parámetros reemplazarán a los que pueda haber indicado en el campo **Línea de comandos para el archivo ejecutable**.

     Esta opción está activada de forma predeterminada.

     La creación y el mantenimiento de la base de datos de Kaspersky está a cargo de nuestros analistas. Cada vez que agregan una aplicación a la base de datos, los analistas de Kaspersky determinan cuáles son sus parámetros de instalación óptimos. Los parámetros se eligen para garantizar que la aplicación pueda instalarse sin problemas en un dispositivo cliente remoto. La base de datos se actualiza automáticamente en el Servidor de administración cuando se ejecuta la tarea del Servidor de administración Descargar actualizaciones en el repositorio.

   Se inicia el proceso para crear el paquete de instalación personalizada.

   El asistente le informará cuando finalice el proceso.

   Si no se crea el paquete de instalación personalizada, se muestra el mensaje adecuado.

7. Haga clic en el botón **Finalizar** para cerrar el asistente.

El paquete de instalación que ha creado se descarga en la subcarpeta Paquetes de la carpeta compartida del Servidor de administración. Después de la descarga, el paquete de instalación personalizada aparece en la lista de paquetes de instalación.

En la lista de paquetes de instalación en el Servidor de administración, puede ver y editar las propiedades del paquete de instalación personalizada.

## Ver y editar propiedades de paquetes de instalación personalizada

Después de crear un paquete de instalación personalizada, puede ver información general sobre el paquete de instalación y especificar la configuración de instalación en la ventana de propiedades.

*Ver y editar propiedades de paquetes de instalación personalizada:*

1. En el árbol de la consola, seleccione el **Servidor de administración** → **Avanzado** → **Instalación remota** → **Paquetes de instalación**.

   Se muestra una lista de paquetes de instalación disponibles en el Servidor de administración.

2. Abra el menú contextual del paquete de instalación y seleccione **Propiedades**.

   Se abrirá la ventana de propiedades del paquete de instalación seleccionado.

3. Ver la siguiente información:

   - Nombre del paquete de instalación
   - Nombre de la aplicación empaquetada en el paquete de instalación personalizada
   - Versión de la aplicación
   - Fecha de creación del paquete de instalación
   - Ruta al paquete de instalación personalizada en el Servidor de administración
   - Línea de comandos del archivo ejecutable

4. Configure los siguientes ajustes:

   - Nombre del paquete de instalación
   - **Instalar los componentes requeridos y generales del sistema**

     Si esta opción está habilitada, antes de que se instale una actualización, la aplicación instalará automáticamente todos los componentes generales del sistema que la actualización requiera para instalarse (los llamados "requisitos previos"). Una actualización podría requerir, por ejemplo, que esté instalada cierta actualización del sistema operativo.

     Si esta opción está deshabilitada, posiblemente tenga que instalar los requisitos previos manualmente.

     Esta opción está deshabilitada de forma predeterminada.

     Esta opción solo está disponible cuando Kaspersky Security Center reconoce la aplicación añadida al paquete de instalación.

   - **Línea de comandos para el archivo ejecutable**

     Si la aplicación requiere un parámetro adicional para instalarse en modo silencioso, especifíquelo en este campo. Para más detalles, consulte la documentación del proveedor.

     También puede introducir otros parámetros.

     Esta opción solo está disponible para los paquetes que no se crean sobre la base de las aplicaciones de Kaspersky.

5. Haga clic en el botón **Aceptar** o **Aplicar** para guardar los cambios, si los hubiera.

Se guardan las nuevas configuraciones.

## Obtención del paquete de instalación del Agente de red del kit de distribución de Kaspersky Security Center

Puede obtener el paquete de instalación del Agente de red del kit de distribución de Kaspersky Security Center sin necesidad de instalar Kaspersky Security Center. Luego, puede usar el paquete de instalación para instalar el Agente de red en los dispositivos cliente.

*Para obtener el paquete de instalación del Agente de red del kit de distribución de Kaspersky Security Center, haga lo siguiente:*

1. Inicie el archivo ejecutable ksc_<número de versión>.<número de compilación>_full_<idioma de localización>.exe del kit de distribución de Kaspersky Security Center.
2. En la ventana que se abre, haga clic en el enlace **Extraer paquetes de instalación**.
3. En la lista de paquetes de instalación, seleccione la casilla de verificación junto al paquete de instalación del Agente de red y haga clic en el botón **Siguiente**.
4. Si es necesario, haga clic en el botón **Examinar** para cambiar la carpeta mostrada para extraer el paquete de instalación.
5. Haga clic en el botón **Extraer**.

   La aplicación extrae el paquete de instalación del Agente de red.
6. Una vez completado el proceso, haga clic en el botón **Cerrar**.

El paquete de instalación del Agente de red se extrae a la carpeta seleccionada.

Puede usar el paquete de instalación para instalar el Agente de red a través de uno de los siguientes métodos:

- Localmente ejecutando el archivo setup.exe de la carpeta extraída
- Mediante instalación silenciosa
- Mediante directivas de grupo de Microsoft Windows

## Distribución de paquetes de instalación a servidores de administración secundarios

*Para distribuir paquetes de instalación a servidores de administración secundarios:*

1. Establezca conexión con el Servidor de administración que controla los servidores de administración secundarios pertinentes.

2. Utilizando uno de estos métodos, cree una tarea para distribuir los paquetes de instalación a los servidores de administración secundarios:

   - Si desea crear una tarea para los servidores de administración secundarios del grupo de administración seleccionado, inicie la creación de una tarea de grupo para ese grupo.

   - Si desea crear una tarea para servidores de administración secundarios específicos, inicie la creación de una tarea para dispositivos específicos.

   Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente.

   En la ventana **Seleccione el tipo de tarea** del Asistente para crear nueva tarea, en el nodo **Servidor de administración de Kaspersky Security Center**, en la carpeta **Avanzado**, seleccione la tarea **Desinstalar paquete de instalación**.

   El Asistente para crear nueva tarea creará la tarea de distribución de los paquetes de instalación seleccionados en los Servidores de administración secundarios específicos.

3. Ejecute la tarea manualmente o espere a que se inicie a consecuencia de la programación configurada para la tarea.

Los paquetes de instalación seleccionados se copiarán a los servidores de administración secundarios específicos.

## Distribución de paquetes de instalación a través de los puntos de distribución

Puede usar puntos de distribución para distribuir los paquetes de instalación en un grupo de administración.

Después de recibir los paquetes de instalación desde el Servidor de administración, los puntos de distribución los distribuyen automáticamente a los dispositivos cliente utilizando la multidifusión IP. La multidifusión del IP de paquetes de instalación nuevos en un grupo de administración ocurre una vez. Si se desconectó un dispositivo cliente de la red corporativa durante la sesión de distribución, el Agente de red de ese dispositivo cliente descarga automáticamente el paquete de instalación relevante desde el punto de distribución cuando se inicia la tarea de instalación.

# Transferir los resultados de la instalación de aplicaciones a Kaspersky Security Center

Después de crear el paquete de instalación de la aplicación, puede configurarlo para que toda la información de diagnóstico sobre los resultados de la instalación de la aplicación se transfiera a Kaspersky Security Center. Para los paquetes de instalación de las aplicaciones de Kaspersky, la transferencia de información sobre los resultados de la instalación de la aplicación se configura de manera predeterminada, sin requerirse ninguna configuración adicional.

*Para configurar la transferencia de información de diagnóstico sobre los resultados de la instalación de la aplicación a Kaspersky Security Center:*

1. Navegue hasta la carpeta del paquete de instalación creado con Kaspersky Security Center para la aplicación seleccionada. La carpeta se puede encontrar en la carpeta compartida especificada durante la instalación de Kaspersky Security Center.

2. Abra el archivo con la extensión .kpd o .kud para editarlos (por ejemplo, en el editor Bloc de notas de Microsoft Windows).

   El archivo tiene el formato de un archivo de configuración .ini normal.

3. Agregue las siguientes líneas al archivo:

   ```
   [SetupProcessResult]
   Wait=1
   ```

   Este comando configura Kaspersky Security Center para que espere a que finalice la instalación de la aplicación para la que se creó el paquete de instalación y analiza el código de devolución del instalador. Si debe deshabilitar la transferencia de datos de diagnóstico, asigne el valor 0 a la clave "Wait".

4. Agregue la descripción de los códigos de devolución para una correcta instalación. Para ello, agregue las siguientes líneas al archivo:

   ```
   [SetupProcessResult_SuccessCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
        …
   ```

   > Los corchetes contienen teclas opcionales.

   Sintaxis de las líneas:

   - `<return code>`. Cualquier número correspondiente al código de devolución del instalador. El número de códigos de devolución puede ser arbitraria.

   - `<description>`. Descripción del texto del resultado de la instalación. Se puede omitir la descripción.

5. Agregue la descripción de los códigos de devolución en caso de una instalación incorrecta. Para ello, agregue las siguientes líneas al archivo:

   ```
   [SetupProcessResult_ErrorCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   ...
   ```

   La sintaxis de estas líneas es igual a la sintaxis de las líneas que contienen los códigos de devolución de una instalación correcta.

6. Cierre el archivo .kpd o .kud cuando guarde todos los cambios.

Por último, los resultados de instalación de la aplicación definida por el usuario se registrarán en los registros de Kaspersky Security Center y aparecerá en la lista de los eventos, en los informes y en los registros de ejecución de tareas.

## Definición de la dirección del servidor proxy de KSN para los paquetes de instalación

En caso de que cambie la dirección o el dominio del Servidor de administración, puede definir la dirección del servidor proxy de KSN para el paquete de instalación.

*Para definir la dirección del servidor proxy de KSN para el paquete de instalación, haga lo siguiente:*

1. En el árbol de la consola, en la carpeta **Instalación remota**, haga doble clic en la subcarpeta **Paquetes de instalación**.
2. En el menú que se abre, seleccione **Propiedades**.
3. En la ventana de propiedades que se abre, seleccione la subsección **General**.
4. En la subsección **General** de la ventana de propiedades, introduzca la dirección del servidor proxy de KSN.

Los paquetes de instalación utilizarán esta dirección como predeterminada.

# Recibir versiones actualizadas de las aplicaciones

Kaspersky Security Center le permite recibir versiones actualizadas de las aplicaciones corporativas almacenadas en los servidores de Kaspersky.

*Para recibir versiones actualizadas de aplicaciones corporativas de Kaspersky:*

1. Realice una de las siguientes acciones:

   - En el árbol de la consola, seleccione el nodo con el nombre del Servidor de administración requerido, asegúrese de que se selecciona la pestaña **Supervisión** y en la sección **Despliegue** haga clic en el enlace **Hay nuevas versiones de las aplicaciones de Kaspersky disponibles**.

     El vínculo **Hay nuevas versiones de las aplicaciones de Kaspersky disponibles** se vuelve visible cuando el Servidor de administración encuentra una nueva versión de una aplicación corporativa en un servidor Kaspersky.

   - En el árbol de la consola, seleccione **Avanzado → Instalación remota → Paquetes de instalación** y en el espacio de trabajo, haga clic en **Acciones adicionales** y de la lista desplegable, seleccione **Ver versiones actuales de las aplicaciones de Kaspersky**.

   Se muestra la lista de la versión actual de la aplicación de Kaspersky.

2. Puede filtrar la lista de aplicaciones de Kaspersky para ayudarse a encontrar la aplicación que busca.

   En la parte superior de la ventana **Versiones actuales de las aplicaciones**, haga clic en el vínculo **Filtro** para filtrar la lista de aplicaciones según los siguientes criterios:

   - **Componentes**. Utilice este criterio para filtrar la lista de aplicaciones de Kaspersky por las áreas de protección que se usan en su red.
   - **Tipo de software descargado**. Utilice este criterio para filtrar la lista de aplicaciones de Kaspersky por tipo de aplicación.
   - **Productos de software y actualizaciones que deben mostrarse**. Utilice este criterio para mostrar las aplicaciones de Kaspersky disponibles según versiones específicas.
   - **Idioma mostrados para software y actualizaciones**. Utilice este criterio para mostrar las aplicaciones de Kaspersky con un idioma de localización específico.

   Haga clic en el botón **Aplicar** para aplicar los filtros seleccionados.

3. Seleccione la aplicación requerida de la lista.

4. Descargue el paquete de distribución de aplicaciones. Para ello, haga clic en el vínculo de la línea **Dirección web del paquete de distribución**.

   Las actualizaciones para las aplicaciones administradas pueden requerir que la versión de Kaspersky Security Center instalada sea posterior a una versión en particular. Si está utilizando una versión anterior a la necesaria, podrá ver estas actualizaciones, pero no las podrá aprobar. Tampoco podrá crear paquetes de instalación a partir de esas actualizaciones hasta que actualice Kaspersky Security Center. Si intenta hacerlo, se le pedirá que actualice su copia de Kaspersky Security Center a la versión mínima requerida.

Si se muestra el botón **Descargar aplicaciones y crear paquetes de instalación** para la aplicación seleccionada, puede hacer clic en este botón para descargar el paquete de distribución de la aplicación y crear un paquete de instalación de manera automática. Kaspersky Security Center descarga el paquete de distribución de aplicaciones al Servidor de administración, en la carpeta compartida especificada durante la instalación de Kaspersky Security Center. El paquete de instalación creado automáticamente se muestra en la carpeta **Instalación remota** del árbol de consola, en la subcarpeta **Paquetes de instalación**.

Después de que la ventana **Versiones actuales de las aplicaciones** se cierra, el enlace **Hay nuevas versiones de las aplicaciones de Kaspersky disponibles** desaparece de la sección **Despliegue**.

Se pueden crear paquetes de instalación para las nuevas versiones de las aplicaciones y administrar los paquetes de instalación recién creados en la carpeta **Instalación remota** del árbol de consola, en la subcarpeta **Paquetes de instalación**.

También se puede abrir la ventana **Versiones actuales de las aplicaciones** al hacer clic en el enlace **Ver versiones actuales de las aplicaciones de Kaspersky** en el espacio de trabajo de la carpeta **Paquetes de instalación**.

# Preparar un dispositivo Windows para la instalación remota

Es posible que la instalación remota de la aplicación en el dispositivo cliente se complete con un error por los siguientes motivos:

- La tarea ya se ha ejecutado correctamente en este dispositivo.

  En este caso, no es necesario volver a realizar la tarea.

- El dispositivo se apaga al iniciarse una tarea.

  En ese caso, encienda el dispositivo y vuelva a iniciar la tarea.

- No hay conexión entre el Servidor de administración y el Agente de red instalado en el dispositivo cliente.

  Para determinar la causa del problema, use la utilidad diseñada para realizar diagnósticos remotos en los dispositivos cliente (klactgui).

- Si no hay un Agente de red instalado en el dispositivo, pueden ocurrir los siguientes problemas durante la instalación remota:

  - El dispositivo cliente tiene **Deshabilitar el uso compartido simple de archivos** habilitado.
  - El servicio del servidor no se está ejecutando en el dispositivo cliente.
  - Los puertos requeridos están cerrados en el dispositivo cliente.
  - La cuenta utilizada para ejecutar la tarea no cuenta con los privilegios suficientes.

  Para evitar problemas que puedan ocurrir durante la instalación de la aplicación en un dispositivo cliente sin Agente de red instalado, debe proceder como se describe en el despliegue forzado a través de la tarea de instalación remota de Kaspersky Security Center.

Antes se usaba la utilidad riprep a fin de preparar un dispositivo de Windows para la instalación remota. Ahora se trata de un método obsoleto para configurar sistemas operativos. No se recomienda el uso de la utilidad riprep en sistemas operativos más nuevos que Windows XP y Windows Server 2003 R2.

# Preparación de un dispositivo Linux e instalación del Agente de red en un dispositivo Linux de forma remota

La instalación del Agente de red consta de dos pasos:

- Preparación de un dispositivo Linux
- Instalación remota del Agente de red

## Preparación de un dispositivo Linux

*Para preparar un dispositivo que ejecute Linux para la instalación remota del Agente de red:*

1. Asegúrese de que el dispositivo en el que desea instalar Network Agent for Linux cuente con una de las distribuciones de Linux compatibles.
2. Descargue el paquete de instalación del Agente de red mediante la interfaz de la aplicación o desde el sitio web de Kaspersky.
3. Asegúrese de que el siguiente software esté instalado en el dispositivo Linux de destino:
   - Sudo (para Ubuntu 10.04, la versión de Sudo 1.7.2p1 o posterior)
   - Intérprete del lenguaje Perl versión 5.10 o posterior
   - utilidad ps

4. Pruebe la configuración del dispositivo:

   a. Compruebe si puede conectarse al dispositivo mediante un cliente SSH (por ejemplo, PuTTY).

      Si no puede conectarse al dispositivo, abra el archivo `/etc/ssh/sshd_config` y asegúrese de que las siguientes configuraciones tengan los valores respectivos que se enumeran a continuación:

      ```
      PasswordAuthentication no
      ChallengeResponseAuthentication yes
      ```

      > No modifique el archivo /etc/ssh/sshd_config si puede conectarse al dispositivo sin problemas; de lo contrario, es posible que se produzca un error de autenticación SSH al ejecutar una tarea de instalación remota.

      Guarde el archivo (si es necesario) y reinicie el servicio SSH utilizando el comando `sudo service ssh restart`.

   b. Deshabilite la contraseña de sudo para la cuenta de usuario con la cual se conectará el dispositivo.

   c. Utilice el comando `visudo` en sudo para abrir el archivo de configuración de sudoers.

      En el archivo que abrió, agregue la siguiente línea al final del archivo: <`nombre de usuario`> `ALL = (ALL) NOPASSWD: ALL`. En este caso, <`nombre de usuario`> es la cuenta de usuario que se utilizará para la conexión del dispositivo mediante SSH. Si está utilizando el sistema operativo Astra Linux, en el archivo /etc/sudoers, agregue la última línea con el siguiente texto: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

   d. Guarde el archivo sudoers y, luego, ciérrelo.

   e. Conéctese nuevamente al dispositivo a través de SSH y asegúrese de que el servicio Sudo no le solicite que ingrese una contraseña; puede hacerlo usando el comando `sudo whoami`.

5. Abra el archivo `/etc/systemd/logind.conf` y luego realice una de las siguientes acciones:

   - Especifique "no" como valor para la configuración KillUserProcesses: `KillUserProcesses=no`.
   - Para la configuración KillExcludeUsers, escriba el nombre de usuario de la cuenta con la que se realizará la instalación remota, por ejemplo, `KillExcludeUsers=root`.

   Si el dispositivo de destino ejecuta Astra Linux, agregue la cadena `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` en el archivo `/home/<nombre de usuario>/.bashrc`, donde <`nombre de usuario`> es la cuenta de usuario que se utilizará para la conexión del dispositivo mediante SSH.

   Para aplicar el ajuste modificado, reinicie el dispositivo Linux o ejecute el siguiente comando:

   ```
   sudo systemctl restart systemd-logind.service
   ```

6. Si desea instalar el Agente de red en dispositivos con el sistema operativo SUSE Linux Enterprise Server 15, primero, instale el paquete insserv-compat para configurar el Agente de red.

7. Si desea instalar el Agente de red en dispositivos con el sistema operativo Astra Linux que se ejecuta en el modo de entorno de software cerrado, lleve a cabo los pasos adicionales para preparar los dispositivos Astra Linux.

8. Si desea instalar el Agente de Red en dispositivos que utilicen el sistema operativo RED OS 7.3.4 o posterior, o MSVSPHERE 9.2 o posterior, instale el paquete libxcrypt-compat para el correcto funcionamiento del Agente de Red.

### Instalación remota del Agente de red

*Para instalar el Agente de red en dispositivos Linux de manera remota:*

1. Descargue y cree un paquete de instalación:

   a. Antes de iniciar la instalación del paquete en el dispositivo, asegúrese de que ya tiene instaladas todas las dependencias (programas y bibliotecas) para este paquete.

   Puede ver las dependencias de cada paquete por su propia cuenta, mediante las utilidades específicas de la distribución Linux en la que se instalará el paquete. Para obtener más información sobre las utilidades, consulte la documentación de su sistema operativo.

   b. Para crear un paquete de instalación remota, use los archivos siguientes:

   - klnagent.kpd
   - akinstall.sh
   - Paquete .deb o .rpm de Agente de red

2. Cree una tarea de instalación remota con la configuración siguiente:

   - En la página **Configuración** del Asistente para crear nueva tarea, seleccione la casilla **Uso de los recursos del sistema operativo a través del Servidor de administración**. Quite la selección a todo.
   - En la página **Seleccione una cuenta para ejecutar la tarea**, especifique la configuración de la cuenta de usuario que se utiliza para la conexión del dispositivo mediante SSH.

3. Ejecute la tarea de instalación remota. Utilice la opción para el comando `su` para preservar el entorno: `-m, -p, --preserve-environment`.

## Preparación de un dispositivo que ejecuta SUSE Linux Enterprise Server 15 para la instalación del Agente de red

*Para instalar el Agente de red en un dispositivo con el sistema operativo SUSE Linux Enterprise Server 15:*

Antes de la instalación del Agente de red, ejecute el siguiente comando:

```
sudo zypper install insserv-compat
```

Esto permite instalar el paquete insserv-compat y configurar el Agente de red correctamente.

> Ejecute el comando `rpm -q insserv-compat` para comprobar si el paquete ya está instalado.

Si su red incluye muchos dispositivos que ejecutan SUSE Linux Enterprise Server 15, puede usar el software especial para configurar y administrar la infraestructura de la empresa. Al usar este software, puede instalar automáticamente el paquete insserv-compat en todos los dispositivos necesarios al mismo tiempo. Por ejemplo, puede usar Puppet, Ansible o Chef, o puede crear su propio script; use cualquier método que sea conveniente para usted.

Si el dispositivo no tiene las claves de firma GPG para SUSE Linux Enterprise, puede aparecer la siguiente advertencia: `Package header is not signed!` Seleccione la opción `i` para ignorar la advertencia.

Además de la instalación del paquete insserv-compat, asegúrese de haber preparado completamente sus dispositivos Linux. Después de eso, implemente e instale el Agente de red.

# Preparación de un dispositivo de macOS para instalación remota de Agente de red

*Para preparar un dispositivo que ejecute macOS para la instalación remota del Agente de red:*

1. Asegúrese de que sudo esté instalado en el dispositivo macOS de destino.

2. Pruebe la configuración del dispositivo:

   a. Asegúrese de que el puerto 22 esté abierto en el dispositivo cliente. Para ello, en las **Preferencias del sistema**, abra el panel **Uso compartido** y asegúrese de que la casilla **Inicio de sesión remoto** esté seleccionada.

   Puede conectarse al dispositivo cliente mediante Secure Shell (SSH) solo a través del puerto 22. No puede cambiar el número de puerto.

   Puede utilizar el comando `ssh <nombre_del_dispositivo>` para iniciar sesión en el dispositivo macOS de forma remota. Para definir quiénes podrán acceder al dispositivo macOS, utilice la opción **Permitir acceso a** del panel **Compartir**.

   b. Deshabilite la contraseña de sudo para la cuenta de usuario con la cual se conectará el dispositivo.

   Utilice el comando `sudo visudo` en la Terminal para abrir el archivo de configuración de sudoers. En el archivo que abrió, en la entrada `Especificación de privilegios de usuario`, especifique lo siguiente: `username ALL = (ALL) NOPASSWD: ALL`. En este caso, `username` representa la cuenta de usuario que se utilizará para la conexión del dispositivo mediante SSH.

   c. Guarde el archivo sudoers y, luego, ciérrelo.

   d. Conéctese nuevamente al dispositivo a través de SSH y asegúrese de que el servicio Sudo no le solicite que ingrese una contraseña; puede hacerlo usando el comando `sudo whoami`.

3. Descargue y cree un paquete de instalación:

   a. Use uno de estos métodos para obtener el paquete de instalación del Agente de red:

      - En el árbol de la consola, abra el menú contextual de **Instalación remota** → **Paquetes de instalación**, haga clic en **Mostrar las versiones actuales de las aplicaciones** y elija uno de los paquetes disponibles.
      - Descargue la versión relevante del Agente de red del sitio web del Servicio de soporte técnico, https://support.kaspersky.com/.
      - Solicite el paquete de instalación a nuestros especialistas del servicio de soporte técnico.

   b. Para crear un paquete de instalación remota, use los archivos siguientes:

      - klnagent.kud
      - install.sh
      - klnagentmac.dmg

4. Cree una tarea de instalación remota con la configuración siguiente:

   - En la página **Configuración** del Asistente para crear nueva tarea, seleccione la casilla **Con los recursos del sistema operativo a través del Servidor de administración**. Quite la selección a todo.
   - En la página **Seleccione una cuenta para ejecutar la tarea**, para ejecutar la tarea, especifique la configuración de la cuenta de usuario que se utiliza para conectar el dispositivo mediante SSH.

El dispositivo cliente está listo para la instalación remota del Agente de red a través de la tarea correspondiente que ha creado.

# Aplicaciones de Kaspersky: licencias y activación

Esta sección describe las funciones de Kaspersky Security Center relacionadas con el manejo de claves de licencia de las aplicaciones administradas de Kaspersky.

Kaspersky Security Center le permite realizar una distribución centralizada de las claves de licencia de las aplicaciones de Kaspersky en dispositivos cliente, supervisar su uso y renovar las licencias.

Al agregar una clave de licencia mediante Kaspersky Security Center, las propiedades de la clave de licencia se guardan en el Servidor de administración. Los parámetros definidos en las propiedades de las claves de licencia permiten que la aplicación genere un informe sobre el uso de las claves de licencia, mantenga al administrador al tanto de la caducidad de las licencias y le informe si se infringe una restricción dispuesta por una licencia. Puede configurar notificaciones sobre el uso de las claves de licencia en los ajustes del Servidor de administración.

# Licencias de aplicaciones administradas

Las aplicaciones de Kaspersky instaladas en los dispositivos administrados se deben licenciar aplicando un archivo de clave o código de activación a cada una de las aplicaciones. Los archivos de clave o códigos de activación se pueden desplegar de las siguientes formas:

- Despliegue automático
- Usar el paquete de instalación de la aplicación administrada
- La tarea *Agregar clave de licencia* para una aplicación administrada
- Activar la aplicación administrada manualmente

Puede agregar una nueva clave de licencia activa o de reserva mediante cualquiera de los métodos enumerados anteriormente. Una aplicación de Kaspersky utiliza una clave activa en el momento actual y almacena una clave de reserva para aplicar después de que caduque la clave activa. La aplicación para la que agrega una clave de licencia define si la clave está activa o si es de reserva. La definición de la clave no depende del método que utilice para agregar una nueva clave de licencia.

## Despliegue automático

Si usa diferentes aplicaciones administradas y tiene que desplegar un archivo de clave o un código de activación específicos en los dispositivos, opte por otras formas de desplegar ese código de activación o archivo de clave.

Kaspersky Security Center le permite desplegar las claves de licencia disponibles a los dispositivos automáticamente. Suponga, por ejemplo, que tiene tres claves de licencia en el repositorio del Servidor de administración. Ha seleccionado la casilla de verificación **Distribuir la clave de licencia automáticamente a los dispositivos administrados** para las tres claves de licencia. Los dispositivos de su organización tienen instalada una aplicación de seguridad de Kaspersky (por ejemplo, Kaspersky Endpoint Security para Windows). Se detecta un nuevo dispositivo al que se debe desplegar una clave de licencia. La aplicación determina, por ejemplo, que dos de las claves de licencia del repositorio se pueden desplegar en el dispositivo: una clave de licencia llamada *Clave_1* y una clave de licencia llamada *Clave_2*. Una de estas claves de licencia se despliega al dispositivo. En este caso, no se puede predecir cuál de las dos claves de licencia se desplegará en el dispositivo porque el despliegue automático de claves de licencia no proporciona ninguna actividad de administrador.

Cuando se despliega una clave de licencia, los dispositivos se vuelven a contar para esa clave de licencia. Debe asegurarse de que la cantidad de dispositivos a los que se desplegó la clave de licencia no exceda el límite de la licencia. Si la cantidad de dispositivos excede el límite de la licencia, a todos los dispositivos que no estaban cubiertos por la licencia se les asignará el estado *Crítico*.

Antes del despliegue, se deben agregar el archivo de clave o el código de activación al repositorio del Servidor de administración.

Instrucciones:

- Consola de administración:
  - Agregar una clave de licencia al repositorio del Servidor de administración
  - Distribución automática de una clave de licencia

  o
- Kaspersky Security Center Web Console:
  - Agregar una clave de licencia al repositorio del Servidor de administración
  - Distribución automática de una clave de licencia

Tenga en cuenta que una clave de licencia distribuida automáticamente podría no aparecer en el repositorio del Servidor de administración virtual en los siguientes casos:

- La clave de licencia no es válida para la aplicación.
- El Servidor de administración virtual no tiene ningún dispositivo administrado.
- La clave de licencia ya ha sido utilizada para dispositivos administrados asociados a otro Servidor de administración virtual y se ha alcanzado el límite a la cantidad de dispositivos.

## Adición de un archivo de clave o un código de activación al paquete de instalación de una aplicación administrada

Por motivos de seguridad, no se recomienda utilizar esta opción. El archivo de clave o el código de activación añadidos a un paquete de instalación pueden verse comprometidos.

Si instala una aplicación administrada con un paquete de instalación, puede especificar un código de activación o un archivo de clave en este paquete de instalación o en la directiva de la aplicación. En ese caso, la clave de licencia se desplegará a los dispositivos administrados cuando estos se sincronicen nuevamente con el Servidor de administración.

Instrucciones:

- Consola de administración:
  - Creación del paquete de instalación
  - Instalar aplicaciones en dispositivos cliente

  o
- Kaspersky Security Center Web Console: Adición de una clave de licencia a un paquete de instalación

### Despliegue con la tarea “Agregar clave de licencia” para una aplicación administrada

Si opta por usar la tarea *Agregar clave de licencia* para una aplicación administrada, puede seleccionar la clave que debe distribuirse a los dispositivos y seleccionar los dispositivos con comodidad, por ejemplo, seleccionando un grupo de administración o una selección de dispositivos.

Antes del despliegue, se deben agregar el archivo de clave o el código de activación al repositorio del Servidor de administración.

Instrucciones:

- Consola de administración:
  - Agregar una clave de licencia al repositorio del Servidor de administración
  - Distribución de claves de licencia a dispositivos cliente

  o
- Kaspersky Security Center Web Console:
  - Agregar una clave de licencia al repositorio del Servidor de administración
  - Distribución de claves de licencia a dispositivos cliente

### Agregar un código de activación o un archivo de clave en los dispositivos manualmente

Puede activar la aplicación de Kaspersky en forma local, usando las herramientas disponibles en la interfaz de la aplicación. Consulte la documentación de la aplicación instalada.

## Visualización de información sobre las claves de licencia en uso

*Para ver información sobre las claves de licencia en uso,*

En el árbol de consola, seleccione la carpeta **Licencias de Kaspersky**.

El espacio de trabajo de la carpeta muestra una lista de las claves de licencia utilizadas en los dispositivos cliente.

Junto a cada una de las claves de licencia se muestra un icono que corresponde al tipo de uso:

-  — Se ha recibido información sobre la clave de licencia actualmente en uso desde un dispositivo cliente conectado al Servidor de administración. El archivo de esta clave de licencia se almacena fuera del Servidor de administración.
-  —La clave de licencia se almacena en el repositorio del Servidor de administración. La distribución automática se encuentra deshabilitada para esta clave de licencia.
-  —La clave de licencia se almacena en el repositorio del Servidor de administración. La distribución automática se encuentra habilitada para esta clave de licencia.

Puede ver información sobre qué claves de licencia se utilizan para activar la aplicación en un dispositivo cliente, si abre la sección **Aplicaciones** de la ventana de propiedades del dispositivo cliente.

Para definir la configuración actualizada de las claves de licencia del Servidor de administración virtual, este envía una solicitud a los servidores de activación de Kaspersky como mínimo una vez al día. Si los servidores DNS configurados en el sistema no permiten acceder a los servidores de Kaspersky, la aplicación utiliza servidores DNS públicos.

Si se recibe una clave de licencia de un dispositivo cliente, no podrá exportarla a un archivo.

# Agregar una clave de licencia al repositorio del Servidor de administración

*Para agregar una clave de licencia al repositorio del Servidor de administración:*

1. En el árbol de consola, seleccione la carpeta **Licencias de Kaspersky**.
2. Comience la tarea de incorporación de claves de licencia mediante uno de los siguientes métodos:
   - Seleccione **Agregar código de activación o archivo de clave** en el menú contextual de la lista de claves de licencia.
   - Haga clic en el enlace **Agregar código de activación o archivo de clave** del espacio de trabajo de la lista de claves de licencia.
   - Haga clic en el botón **Agregar código de activación o archivo de clave**.

   Se inicia el asistente Asistente para agregar claves de licencia.
3. Seleccione cómo desea activar el Servidor de administración: usando un código de activación o usando un archivo de clave.
4. Especifique su código de activación o un archivo de clave.
5. Seleccione la opción **Distribuir la clave de licencia automáticamente a los dispositivos administrados** si desea distribuir de manera inmediata una clave de licencia relevante en su red. Si no selecciona esta opción, puede distribuir una clave de licencia manualmente más adelante.

   Como consecuencia, se descarga el archivo de clave y Asistente para agregar claves de licencia finaliza. Ahora, puede ver la clave de licencia agregada en la lista de licencias de Kaspersky.

# Eliminar una clave de licencia del Servidor de administración

*Para eliminar una clave de licencia del Servidor de administración:*

1. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
2. En la ventana de propiedades del Servidor de administración que se abre, seleccione la sección **Claves de licencia**.
3. Elimine la clave de licencia al hacer clic en el botón **Eliminar**.

   Al hacer esto, se elimina la clave de licencia.

Si agregó una clave de licencia de reserva, al eliminar la clave de licencia activa, la clave de reserva se convertirá automáticamente en la clave de licencia activa.

Después de que se haya eliminado la clave de licencia activa del Servidor de administración, las funciones Administración de vulnerabilidades y parches y Administración de dispositivos móviles no están disponibles. Puede volver a agregar una clave de licencia eliminada o agregar una clave de licencia nueva.

# Distribución de claves de licencia a dispositivos cliente

Kaspersky Security Center permite distribuir una clave de licencia a los dispositivos cliente mediante la tarea de *distribución de claves de licencia*.

Antes de realizar la distribución, agregue la clave de licencia al repositorio del Servidor de administración.

*Para distribuir una clave de licencia a sus dispositivos cliente:*

1. En el árbol de consola, seleccione la carpeta **Licencias de Kaspersky**.
2. En el espacio de trabajo de la lista de claves de licencia, haga clic en el botón **Distribuir la clave de licencia automáticamente a los dispositivos administrados**.

   Se inicia el **Asistente para la creación de tareas de activación de aplicaciones**. Avance por el asistente utilizando el botón **Siguiente**.
3. En la lista de aplicaciones, seleccione la aplicación para la que desee crear una tarea.

4. En el paso **Agregar clave** del asistente, agregue la clave de licencia mediante una de las siguientes opciones:

   - Seleccione la opción **Código de activación** para agregar un código de activación del repositorio de Kaspersky Security Center.

     Haga clic en **Seleccionar**. En la ventana que se abre, seleccione el código de activación y, luego, haga clic en **Aceptar**.

   - Seleccione la opción **Archivo de clave o clave** y, a continuación, siga estos pasos:

     a. Haga clic en **Seleccionar**.

     b. En el menú contextual, seleccione una de estas opciones:

     - **$SelectKeyIdDropdownOption1**.

       En la ventana que se abre, seleccione el archivo de clave del dispositivo y haga clic en **Abrir**.

     - **$SelectKeyIdDropdownOption2**.

       En la ventana que se abre, seleccione la clave del repositorio de Kaspersky Security Center y luego haga clic en **Aceptar**.

5. Si desea reemplazar la clave de licencia activa, desmarque la casilla predeterminada **Utilizar como clave de reserva**.

   Por ejemplo, puede ser necesario cuando la organización cambia y se necesita la clave de otra organización en el dispositivo o si la clave se volvió a emitir y la nueva licencia caduca antes que la licencia actual. Para evitar errores, debe desmarcar la casilla **Utilizar como clave de reserva**.

   Si desea obtener más información sobre los problemas que pueden surgir al agregar una clave de licencia a Kaspersky Security Center Windows y cómo resolverlos, consulte la Base de conocimientos de Kaspersky Security Center.

6. Verifique la información de la clave de licencia y luego haga clic en **Siguiente**.

7. En este paso del asistente, seleccione los dispositivos a los que desea asignar la tarea de agregar clave. Puede especificar dispositivos (hasta 1000) de las siguientes maneras:

   - **Seleccionar dispositivos de la red detectados por el Servidor de administración**. En este caso, la tarea se asigna a dispositivos específicos. Estos pueden ser tanto dispositivos asignados a grupos de administración como dispositivos no asignados.

   - **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**. Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

   - **Asignar tarea a una selección de dispositivos**. En este caso, la tarea se asigna a los dispositivos incluidos en una selección creada anteriormente. Puede especificar la selección predeterminada o una personalizada que haya creado.

   - **Asignar tarea a un grupo de administración**. En este caso, la tarea se asigna a los dispositivos incluidos en el grupo de administración creado anteriormente.

8. En el paso **Configurar programación de tarea** del asistente, cree una programación para el inicio de la tarea:

- **Inicio programado**:
  - Una vez

    La tarea se ejecuta una vez, en la fecha y hora especificadas (de manera predeterminada, el día en que se creó la tarea).

  - Manual

    La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

    Esta opción está seleccionada de forma predeterminada.

  - Al descargar nuevas actualizaciones al repositorio

    La tarea se ejecuta después de descargar las actualizaciones en el repositorio. Por ejemplo, es posible que desee utilizar este programa para la tarea de encontrar vulnerabilidades y actualizaciones necesarias.

  - Ante brotes de virus

    La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

    - Antivirus para estaciones de trabajo y servidores de archivos
    - Antivirus para defensa del perímetro
    - Antivirus para sistemas de correo

    Por defecto, están seleccionados todos los tipos de aplicaciones.

    En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

  - Al completarse otra tarea

La tarea actual se iniciará después de que se complete otra tarea. Esta opción solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

- Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
- Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

  De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
- Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

- **Ejecutar tareas no realizadas**

  Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

  Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

  Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

  Esta opción está deshabilitada de forma predeterminada.

- **Esperar un tiempo definido al azar antes de iniciar la tarea**

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

- **Limitar el tiempo de espera a esta cantidad de minutos**

Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

9. En el paso **Defina el nombre de la tarea** del asistente, especifique el nombre de la tarea. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).

10. En la página **Finalizar la creación de la tarea** del asistente, haga clic en el botón **Finalizar** para cerrar el asistente.

    Para que la tarea se inicie en cuanto se cierre el asistente, marque la casilla **Ejecutar la tarea al finalizar el asistente**.

Las tareas creadas mediante el **Asistente para la creación de tareas de activación de aplicaciones** son tareas para dispositivos específicos que se almacenan en la carpeta **Tareas** del árbol de consola.

También puede crear una tarea de distribución de claves de licencia local o de grupo mediante el Asistente para crear nueva tarea para un grupo de administración y para un dispositivo cliente.

# Distribución automática de una clave de licencia

Kaspersky Security Center permite la distribución automática de claves de licencia a dispositivos administrados si están ubicadas en el repositorio de claves de licencia del Servidor de administración. La distribución automática de claves de licencia no se aplica a los dispositivos de la carpeta **Dispositivos no asignados**.

*Para distribuir una clave de licencia en forma automática a los dispositivos administrados:*

1. En el árbol de consola, seleccione la carpeta **Licencias de Kaspersky**.

2. En el espacio de trabajo de la carpeta, seleccione la clave de licencia que desea distribuir a los dispositivos automáticamente.

3. Abra la ventana de propiedades de la clave de licencia seleccionada de una de las siguientes maneras:

   - Seleccionando **Propiedades** en el menú contextual de la clave de licencia.

   - Al hacer clic en el enlace **Ver propiedades de la clave de licencia** en el cuadro de información para la clave de licencia seleccionada.

4. En la ventana de propiedades de la clave de licencia que se abre, active la casilla **Clave de licencia distribuida automáticamente**. Cierre la ventana de propiedades de la clave de licencia.

La clave de licencia se distribuirá automáticamente a todos los dispositivos compatibles.

La distribución de claves de licencia se realiza a través del Agente de red. No se crean tareas de distribución de clave de licencia para la aplicación.

Durante la distribución automática de una clave de licencia, se tiene en cuenta el límite de licencia para el número de dispositivos. (El límite de licencia está indicado en las propiedades de la clave de licencia). Si se alcanza el límite de licencia, la distribución de esta clave de licencia en los dispositivos cesa automáticamente.

El Servidor de administración virtual distribuye automáticamente las claves de licencia desde su repositorio y desde el repositorio del Servidor de administración. Le sugerimos que atienda a las siguientes recomendaciones:

- Use la tarea *Agregar clave de licencia* para seleccionar la clave de licencia que se debe distribuir a los dispositivos.
- Evite deshabilitar la opción **Permitir el despliegue automático de claves de licencia de este Servidor de administración virtual a sus dispositivos** en la configuración del Servidor de administración virtual. De lo contrario, el Servidor de administración virtual no distribuirá claves de licencia a los dispositivos, incluidas las claves de licencia del repositorio del Servidor de administración.

Si selecciona la casilla **Clave de licencia distribuida automáticamente** en la ventana de propiedades de la clave de licencia, se distribuye una clave de licencia en su red de forma inmediata. Si no selecciona esta opción, puede distribuir una clave de licencia manualmente más adelante.

# Crear y ver un informe de uso de claves de licencia

*Para crear un informe de uso de claves de licencia en dispositivos cliente:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la pestaña **Informes**.
3. Seleccione la plantilla del informe llamada **Informe de uso de claves de licencia** o cree una nueva plantilla de informe del mismo tipo.

El espacio de trabajo del informe de uso de claves muestra información acerca de las claves activas y claves de licencia de reserva utilizadas en los dispositivos cliente. El informe también contiene información sobre los dispositivos en los que se usan las claves, y sobre las restricciones especificadas en las propiedades de dichas claves de licencia.

# Ver información sobre las claves de licencia de la aplicación

*Para ver las claves de licencia que se están utilizando para una aplicación de Kaspersky:*

1. En el árbol de consola de Kaspersky Security Center, seleccione el nodo **Dispositivos administrados** y vaya a la pestaña **Dispositivos**.
2. Haga clic con el botón derecho del ratón para abrir el menú contextual del dispositivo relevante y seleccione **Propiedades**.
3. En la ventana que se abre, que contendrá las propiedades del dispositivo, vaya a la sección **Aplicaciones**.

4. En la lista de aplicaciones que aparece, seleccione la aplicación cuyas claves de licencia desea ver y haga clic en el botón **Propiedades**.

5. En la ventana de las propiedades de la aplicación que se abre, seleccione la sección **Claves de licencia**.

   La información que busca se mostrará en el espacio de trabajo de la sección.

## Exportación de un archivo de clave de licencia

Si su clave de licencia se eliminó accidentalmente y desea restaurarla, puede exportar un archivo de clave de licencia desde otro Servidor de administración.

Para exportar un archivo de clave de licencia, debe tener el derecho **Exportar archivo de clave** en el área funcional **Características generales: administración de claves**.

Si se recibe una clave de licencia de un dispositivo cliente, no podrá exportarla.

*Para exportar una clave de licencia:*

1. En el árbol de consola, seleccione la carpeta **Licencias de Kaspersky**.

2. En la lista, seleccione la clave de licencia que desee exportar a un archivo.

3. En el cuadro de información que se abre, haga clic en el vínculo **Exportar archivo de clave**.

4. En la ventana que se abre, especifique la ruta a la carpeta donde desea guardar un archivo de clave de licencia y luego especifique un nombre de archivo. Luego, haga clic en **Guardar**.

El archivo de clave de licencia se exporta a la carpeta seleccionada en el formato .key.

Si la clave de licencia cuyo archivo exportó se agregó al repositorio del Servidor de administración como un código de activación y desea agregar el archivo de clave de licencia exportado al repositorio de otro Servidor de administración, debe agregarlo como un código de activación, no como un archivo de clave. De lo contrario, se producirá un error. Debe abrir el archivo de clave de licencia exportado en cualquier editor de texto conveniente y luego copiar el código de activación.

# Configurar la protección de la red

En esta sección, encontrará información sobre la configuración manual de tareas y directivas, sobre los roles de usuario y sobre la creación de una jerarquía de tareas y una estructura de grupos de administración.

# Procedimiento: Configurar la protección de la red

El asistente de inicio rápido crea directivas y tareas con la configuración predeterminada. Esta configuración podría ser subóptima (o incluso inadmisible) para su organización. Por este motivo, recomendamos que modifique estas directivas y tareas predeterminadas y que, de ser necesario, cree otras directivas y tareas adicionales para su red.

## Requisitos previos

Antes de comenzar, compruebe que hizo lo siguiente:

- Instaló el Servidor de administración de Kaspersky Security Center
- Kaspersky Security Center Web Console instalada (opcional)
- Completado el escenario de instalación principal de Kaspersky Security Center
- Completó todos los pasos del asistente de inicio rápido o creó manualmente las siguientes directivas y tareas en el grupo de administración **Dispositivos administrados**:
  - Directiva de Kaspersky Endpoint Security
  - Tarea de grupo para actualizar Kaspersky Endpoint Security
  - Directiva del Agente de red
  - Tarea *Buscar vulnerabilidades y actualizaciones requeridas*

El proceso para configurar la protección de la red se divide en etapas:

1. **Configurar y propagar directivas y perfiles de directivas para las aplicaciones de Kaspersky**

   Para configurar y propagar la configuración de las aplicaciones Kaspersky instaladas en los dispositivos administrados, puede utilizar dos enfoques de la gestión de la seguridad diferentes: centrada en el dispositivo o centrada en el usuario. Estos dos enfoques también se pueden combinar. Para implementar la administración de seguridad centrada en el dispositivo, puede usar las herramientas proporcionadas en la Consola de administración basada en Microsoft Management Console o en Kaspersky Security Center Web Console. La administración de la seguridad centrada en el usuario solamente se puede implementar a través de Kaspersky Security Center Web Console.

2. **Configurar tareas para administrar las aplicaciones de Kaspersky en forma remota**

   Revise las tareas creadas con el asistente de inicio rápido y modifique sus ajustes según corresponda.

   Instrucciones:

   - Consola de administración:
     - Configuración de la tarea de grupo para actualizar Kaspersky Endpoint Security
     - Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas
   - Kaspersky Security Center Web Console:

- Configuración de la tarea de grupo para actualizar Kaspersky Endpoint Security
- Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

Si es necesario, cree tareas adicionales para administrar las aplicaciones Kaspersky instaladas en los dispositivos cliente.

3. **Evaluar y limitar el impacto de los eventos en la base de datos**

   Se transfiere la información sobre eventos que ocurren durante el funcionamiento de aplicaciones administradas de un dispositivo cliente y se la registra en la base de datos del Servidor de administración. Para reducir la carga en el Servidor de administración, evalúe y limite el número máximo de eventos que se pueden almacenar en la base de datos.

   Instrucciones:

   - Consola de administración: Establecer el número máximo de eventos
   - Kaspersky Security Center Web Console: Configuración del número máximo de eventos

### Resultados

Al concluir este escenario, su red estará protegida a través de la configuración de las aplicaciones de Kaspersky, de las distintas tareas y de los eventos recibidos por el Servidor de administración:

- Las aplicaciones de Kaspersky tendrán la configuración definida en las directivas y en los perfiles de directivas.
- Las aplicaciones se administrarán a través de un grupo de tareas.
- Habrá un límite a la cantidad de eventos almacenados en la base de datos.

Una vez que termine de configurar la protección para su red, asegúrese de que las bases de datos y las aplicaciones de Kaspersky se actualicen en forma periódica.

Para obtener detalles sobre cómo configurar las respuestas automáticas a las amenazas detectadas por Kaspersky Sandbox, consulte la Ayuda en línea de Kaspersky Sandbox 2.0.

## Configuración y propagación de directivas: enfoque centrado en el dispositivo

Cuando complete este proceso, las aplicaciones de sus dispositivos administrados estarán configuradas a través de las directivas y los perfiles de directiva que usted defina.

### Requisitos previos

Antes de comenzar, asegúrese de haber instalado correctamente el Servidor de administración de Kaspersky Security Center y Kaspersky Security Center Web Console (opcional). Si instaló Kaspersky Security Center Web Console, es posible que también desee considerar la administración de seguridad centrada en el usuario como una opción alternativa o adicional al enfoque centrado en el dispositivo.

## Etapas

El proceso para administrar las aplicaciones de Kaspersky utilizando un enfoque centrado en el dispositivo se divide en los siguientes pasos:

1. **Configurar directivas para las aplicaciones**

   Cree y configure una directiva para cada aplicación de Kaspersky que se encuentre instalada en los dispositivos administrados. Estas directivas se propagarán a los dispositivos cliente.

   Cuando se utiliza el asistente de inicio rápido para configurar la protección de la red, Kaspersky Security Center crea una directiva predeterminada para las siguientes aplicaciones:

   - Kaspersky Endpoint Security para Windows (para dispositivos cliente con Windows)
   - Kaspersky Endpoint Security for Linux (para dispositivos cliente con Linux)

   Si completó el proceso de configuración utilizando este asistente, no es necesario que cree una nueva directiva para esta aplicación. Lleve a cabo la configuración manual de la directiva de Kaspersky Endpoint Security.

   Si tiene una estructura jerárquica de varios Servidores de administración o grupos de administración, los Servidores de administración secundarios y los grupos de administración secundarios heredan las directivas del Servidor de administración principal de forma predeterminada. Puede forzar la herencia de los grupos secundarios y los Servidores de administración secundarios para prohibir cualquier modificación de los ajustes configurados en la directiva ascendente. Si desea que solo algunos de los ajustes se hereden por la fuerza, bloquee esos ajustes en la directiva de nivel superior. El resto de configuraciones desbloqueadas estarán disponibles para modificación en las directivas posteriores. La jerarquía de directivas resultante le será de gran utilidad para gestionar los dispositivos de los grupos de administración.

   Instrucciones:

   - Consola de administración: Creación de una directiva
   - Kaspersky Security Center Web Console: Crear una directiva

2. **Crear perfiles de directivas (opcional)**

   Si desea que los dispositivos de un mismo grupo de administración estén sujetos a distintos ajustes de directivas, puede crear perfiles de directivas para esos dispositivos. Un perfil de directiva es un subconjunto nominado de los valores de configuración definidos en una directiva. Este subconjunto de valores, que se distribuye a los dispositivos de destino junto con la propia directiva, entra en vigor cuando se presenta una condición específica, llamada *condición de activación del perfil*. Un perfil contiene solamente los valores de configuración que difieren de los de la directiva "básica" que se encuentra activa en el dispositivo administrado.

   A través de las condiciones de activación, podrá aplicar perfiles de directivas diferentes a, por ejemplo, los dispositivos que pertenezcan a ciertas unidades o a ciertos grupos de seguridad de Active Directory, a los que tengan configuraciones de hardware específicas o a los que estén marcados con etiquetas específicas. Puede usar las etiquetas para filtrar dispositivos que reúnen criterios específicos. Podría, por ejemplo, crear una etiqueta llamada *Windows*, marcar con ella los dispositivos que utilicen el sistema operativo Windows y especificarla como condición de activación para un perfil de directiva. Ello hará que las aplicaciones de Kaspersky instaladas en dispositivos con Windows queden sujetas a un perfil de directiva específico.

   Instrucciones:

   - Consola de administración:
     - Crear un perfil de directiva
     - Crear una regla de activación para un perfil de directiva
   - Kaspersky Security Center Web Console:

- Crear un perfil de directiva
- Crear una regla de activación para un perfil de directiva

3. **Propagar las directivas y los perfiles de directivas a los dispositivos administrados**

   De forma predeterminada, el Servidor de administración se sincroniza automáticamente con los dispositivos administrados cada 15 minutos. Puede evitar la sincronización automática y ejecutar la sincronización manualmente utilizando el comando Forzar sincronización. También se realiza una sincronización forzada cada vez que se crea o modifica una directiva o perfil de directiva. Las directivas nuevas o con cambios y los perfiles de directivas se propagan a los dispositivos administrados durante la sincronización.

   Si usa Kaspersky Security Center Web Console, puede verificar si las directivas y los perfiles de directivas se entregaron a un dispositivo. Kaspersky Security Center especifica la fecha y la hora de entrega en las propiedades del dispositivo.

   Instrucciones:

   - Consola de administración: sincronización forzada
   - Kaspersky Security Center Web Console: Sincronización forzada

### Resultados

Al concluir este proceso, las aplicaciones de Kaspersky tendrán la configuración especificada y propagada a través de la jerarquía de directivas.

Las directivas y los perfiles de directivas configurados para las aplicaciones se aplicarán automáticamente a los nuevos dispositivos que se agreguen a los grupos de administración.

## Acerca de la administración de la seguridad centrada en el dispositivo y centrada en el usuario

Puede administrar los ajustes de seguridad utilizando dos enfoques o perspectivas diferentes. Uno de estos enfoques pone el eje en las características de los dispositivos; el otro, en los roles de los usuarios. El primer enfoque se denomina *administración de la seguridad centrada en el dispositivo*, mientras que el segundo recibe el nombre de *administración de la seguridad centrada en el usuario*. Puede usar cualquiera de estos métodos (o ambos en conjunto) para configurar sus aplicaciones de maneras diferentes en dispositivos diferentes. Para implementar la administración de seguridad centrada en el dispositivo, puede usar las herramientas proporcionadas en la Consola de administración basada en Microsoft Management Console o en Kaspersky Security Center Web Console. La administración de la seguridad centrada en el usuario solamente se puede implementar a través de Kaspersky Security Center Web Console.

El enfoque centrado en el dispositivo permite que la configuración de una aplicación de seguridad varíe según las características del dispositivo administrado en el que se encuentra instalada. Es posible, por ejemplo, definir ajustes de configuración diferentes para dispositivos asignados a grupos de administración diferentes. Los dispositivos también pueden diferenciarse sobre la base de sus especificaciones de hardware o de su uso en Active Directory.

El enfoque centrado en el usuario permite configurar las aplicaciones de seguridad de maneras diferentes para roles de usuario diferentes. Puede crear una serie de roles de usuario, asignarlos a sus usuarios según las funciones que desempeñen en la empresa y luego crear configuraciones diferentes, que se apliquen a uno u otro dispositivo según el rol asignado al propietario del dispositivo. Imagine, por ejemplo, que una aplicación de Kaspersky debe estar configurada de un modo diferente si se encuentra instalada en el dispositivo de un contador o en el dispositivo de un especialista en RR. HH. Al implementar la administración de la seguridad centrada en el usuario, puede hacer que cada departamento (el de Contabilidad y el de Recursos Humanos) tenga su propio "juego de ajustes" para esa aplicación. El juego de ajustes determina qué valores de configuración pueden ser modificados por los usuarios y cuáles se imponen por la fuerza y solamente pueden ser modificados por el administrador.

El enfoque centrado en el usuario también permite configurar una aplicación de un modo específico para un usuario específico. Esto puede ser útil si hay un empleado con un rol único en la empresa o si se quieren supervisar los problemas de seguridad asociados a los dispositivos de una persona en particular. El rol de este empleado en particular podría determinar si la persona tendrá más o menos derechos para modificar los ajustes de la aplicación. Un administrador de sistemas que tenga a su cargo los dispositivos cliente de una oficina local podría necesitar más derechos que otros usuarios.

El enfoque centrado en el dispositivo y el enfoque centrado en el usuario pueden combinarse. Por ejemplo, puede configurar una directiva de aplicación específica para cada grupo de administración y luego crear perfiles de directivas para una o varias funciones de usuario de su empresa. En este caso, las directivas y los perfiles de directiva se aplican en el siguiente orden:

1. Se aplicarán las directivas creadas en el marco del enfoque centrado en el dispositivo.
2. Los perfiles modificarán las directivas siguiendo el orden de prioridad definido para los perfiles de directivas.
3. Los perfiles de directivas vinculados a los roles de usuario modificarán las directivas.

# Configuración manual de la directiva de Kaspersky Endpoint Security

Esta sección proporciona recomendaciones sobre cómo configurar la directiva de Kaspersky Endpoint Security, que es creada por el Asistente de inicio rápido. Puede establecer la configuración en la ventana de propiedades de la directiva.

Cuando modifique un ajuste, recuerde hacer clic en el ícono de bloqueo ubicado sobre el ajuste para poder usar su valor en una estación de trabajo.

## Configuración de la directiva en la sección Protección avanzada contra amenazas

Para obtener una descripción completa de los ajustes disponibles en esta sección, consulte la documentación de Kaspersky Endpoint Security para Windows.

En la sección **Protección avanzada contra amenazas**, puede configurar el uso de Kaspersky Security Network para Kaspersky Endpoint Security para Windows. También puede configurar Kaspersky Endpoint Security para Windows, como detección de comportamiento, prevención de exploits, Prevención de intrusiones en el host y motor de reparación.

En la subsección **Kaspersky Security Network**, le recomendamos que active la opción **Kaspersky Security Network**. Esta función ayuda a redistribuir y optimizar el tráfico de la red. Si la opción **Kaspersky Security Network** está deshabilitada, puede habilitar el uso directo de servidores KSN.

## Configuración de la directiva en la sección Protección básica contra amenazas

Para obtener una descripción completa de los ajustes disponibles en esta sección, consulte la documentación de Kaspersky Endpoint Security para Windows.

En la sección **Protección básica contra amenazas** de la ventana de propiedades de la directiva, le recomendamos que especifique configuraciones adicionales en las subsecciones **Firewall** y **Protección contra amenazas de archivo**.

La subsección **Firewall** contiene ajustes que le permiten controlar la actividad de red de las aplicaciones en los dispositivos cliente. Un dispositivo cliente utiliza una red a la que se le ha asignado alguno de estos estados: pública, local o de confianza. Kaspersky Endpoint Security puede permitir o bloquear el tráfico de red en un dispositivo basándose en el estado de la red. Cuando agregue una nueva red a su organización, deberá asignarle un estado de red adecuado. Si el dispositivo cliente es, por ejemplo, una computadora portátil, recomendamos que el dispositivo use una red pública o de confianza, ya que la computadora portátil no siempre está conectada a la red local. En la subsección **Firewall** puede verificar si ha asignado correctamente estados a las redes utilizadas en su organización.

*Para revisar la lista de redes:*

1. En las propiedades de la directiva, vaya a **Protección básica contra amenazas** → **Firewall**.
2. En la sección **Redes disponibles**, haga clic en el botón **Configuración**.
3. En la ventana **Firewall** que se abre, vaya a la pestaña **Redes** para ver la lista de redes.

En la subsección **Protección contra amenazas de archivo** puede desactivar el análisis de las unidades de red. El análisis de unidades de red puede tener un impacto pronunciado en las unidades. Es preferible realizar análisis indirectos en los servidores de archivos.

*Para deshabilitar el análisis de unidades de red:*

1. En las propiedades de la directiva, vaya a **Protección básica contra amenazas** → **Protección contra amenazas de archivo**.
2. En la sección **Nivel de seguridad**, haga clic en el botón **Configuración**.
3. En la ventana **Protección contra amenazas de archivo** que se abre, en la ficha **General**, desmarque la casilla **Todas las unidades de red**.

## Configuración de la directiva en la sección Configuración general

Para obtener una descripción completa de los ajustes disponibles en esta sección, consulte la documentación de Kaspersky Endpoint Security para Windows.

En la sección **Configuración general** de la ventana de propiedades de la directiva, le recomendamos que especifique configuraciones adicionales en las subsecciones **Informes y repositorios** e **Interfaz**.

En la subsección **Informes y repositorios**, vaya a la sección **Transferencia de datos al Servidor de administración**. La casilla **Acerca de las aplicaciones iniciadas** especifica si la base de datos del Servidor de administración guarda la información sobre todas las versiones de todos los módulos del software en los dispositivos conectados a una red. Si esta casilla está marcada, la información guardada puede requerir una cantidad significativa de espacio en disco en la base de datos de Kaspersky Security Center (docenas de gigabytes). Desactive la casilla **Acerca de las aplicaciones iniciadas** si está activada en la directiva de nivel superior.

Si la Consola de administración administra la protección contra amenazas en la red de la organización en modo centralizado, deshabilite la interfaz de usuario de Kaspersky Endpoint Security para Windows en las estaciones de trabajo. Para ello, en la subsección **Interfaz**, vaya a la sección **Interacción con el usuario** y seleccione la opción **No mostrar interfaz del usuario**.

Para habilitar la protección con contraseña en las estaciones de trabajo, en la subsección **Interfaz**, vaya a la sección **Protección con contraseña**, haga clic en el botón **Configuración** y seleccione la casilla **Habilitar la protección con contraseña**.

# Configuración de la directiva en la sección Configuración de eventos

En la sección **Configuración de eventos**, debe deshabilitar el almacenamiento de cualquier evento en el Servidor de administración, excepto los siguientes:

- En la pestaña **Crítico**:
  - *La autoejecución de la aplicación está deshabilitada*
  - *Acceso denegado*
  - *Inicio de aplicación prohibido*
  - *No se puede desinfectar*
  - *Contrato de licencia de usuario final infringido*
  - *No se pudo cargar el módulo de cifrado*
  - *No se pueden iniciar dos tareas al mismo tiempo*
  - *Se detectó una amenaza activa; ejecute la Desinfección avanzada*
  - *Ataque de red detectado*
  - *No se actualizaron todos los componentes*
  - *Error de activación*
  - *Error al habilitar el modo portátil*
  - *Error de interacción con Kaspersky Security Center*
  - *Error al deshabilitar el modo portátil*
  - *Error al cambiar los componentes de la aplicación*
  - *Error al implementar las reglas de cifrado o descifrado de archivos*
  - *No se puede aplicar la directiva*
  - *Proceso finalizado*
  - *Actividad de red bloqueada*
- En la pestaña **Error funcional**: *La configuración de la tarea no es válida y no se aplicó*

- En la pestaña **Advertencia**:
  - *Autoprotección deshabilitada*
  - *Clave de reserva incorrecta*
  - *El usuario optó por no implementar la directiva de cifrado*
- En la ficha **Información**: *Inicio de aplicación prohibido en el modo de prueba*

# Configuración manual de la tarea de grupo para actualizar Kaspersky Endpoint Security

La opción de programación óptima y recomendada para Kaspersky Endpoint Security versiones 10 y posteriores es **Al descargar nuevas actualizaciones al repositorio** cuando la casilla de verificación **Esperar un tiempo definido al azar antes de iniciar la tarea** está seleccionada.

# Instalación manual de la tarea de grupo para analizar un dispositivo con Kaspersky Endpoint Security

El Asistente de inicio rápido crea una tarea de grupo para analizar un dispositivo. De forma predeterminada, la tarea tiene asignada la programación **Ejecutar los viernes a las 7:00 p. m.** con aleatorización automática y la casilla de verificación **Ejecutar tareas no realizadas** no está marcada.

Esto significa que si los dispositivos de la organización se apagan, por ejemplo, los viernes a las 6:30 p. m., la tarea de análisis de los dispositivos nunca se ejecutará. Debe configurar la programación más cómoda para esta tarea según las reglas del lugar de trabajo adoptadas en la organización.

# Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas

El Asistente de inicio rápido crea la tarea *Buscar vulnerabilidades y actualizaciones requeridas* para el Agente de red. De forma predeterminada, se asigna a la tarea la programación **Ejecutar los martes a las 7:00 p. m.** con aleatorización automática, y la casilla **Ejecutar tareas no realizadas** está marcada.

Si las reglas del lugar de trabajo de la organización especifican el cierre de todos los dispositivos a esta hora, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* se ejecutará después de que los dispositivos se vuelvan a encender; es decir, el miércoles por la mañana. Esto puede ser inconveniente porque los análisis de vulnerabilidades pueden hacer que aumente la carga en los subsistemas de disco y CPU. Debe buscar que la programación de la tarea se adecue a las reglas dispuestas por su organización.

# Configuración manual de la tarea de grupo para la instalación de actualizaciones y la reparación de vulnerabilidades

El Asistente de inicio rápido crea una tarea de grupo para la instalación de actualizaciones y la reparación de vulnerabilidades para el Agente de red. De forma predeterminada, la tarea está configurada para ejecutarse todos los días a la 1:00 a. m. con una demora definida al azar automáticamente, y la opción **Ejecutar tareas no realizadas** no debe estar habilitada.

Si las reglas del lugar de trabajo de la organización especifican el cierre de dispositivos durante la noche, la instalación de actualizaciones nunca se ejecutará. Debe configurar la programación más cómoda para esta tarea de análisis de vulnerabilidades según las reglas del lugar de trabajo adoptadas en la organización. También es importante tener en cuenta que la instalación de actualizaciones puede requerir reiniciar el dispositivo.

# Configuración del número máximo de eventos en el repositorio de eventos

En la sección **Repositorio de eventos** de la ventana de propiedades del Servidor de administración, puede editar la configuración del almacenamiento de eventos en la base de datos del Servidor de administración limitando el número de registros de eventos o el tiempo de almacenamiento de los registros. Cuando se especifica el número máximo de eventos, la aplicación calcula una cantidad aproximada de espacio de almacenamiento requerido para el número especificado. Puede utilizar este cálculo aproximado para evaluar si tiene suficiente espacio libre en el disco para evitar el desbordamiento de la base de datos. La capacidad predeterminada de la base de datos del Servidor de administración es de 400 000 eventos. La capacidad máxima recomendada de la base de datos es de 45 millones de eventos.

La aplicación comprueba la base de datos cada 10 minutos. Si la cantidad de eventos alcanza el valor máximo especificado más 10 000, la aplicación elimina los eventos más antiguos para que solo quede la cantidad máxima de eventos especificada.

Cuando el Servidor de administración elimina los eventos antiguos, no puede guardar los nuevos eventos en la base de datos. Durante este período de tiempo, la información sobre los eventos que fueron rechazados se escribe en el Registro de eventos de Kaspersky. Los nuevos eventos se ponen en cola y se guardan en la base de datos una vez finalizada la operación de borrado.

*Para limitar la cantidad de eventos que se pueden almacenar en el repositorio de eventos en el Servidor de administración:*

1. Haga clic con el botón derecho en el Servidor de administración y luego seleccione **Propiedades**.

   Se abre la ventana Propiedades del Servidor de administración.

2. En el espacio de trabajo de la sección del **Repositorio de eventos**, especifique el número máximo de eventos almacenados en la base de datos.

3. Haga clic en **Aceptar**.

Además, puede cambiar la configuración de cualquier tarea para guardar eventos relacionados con el progreso de la misma, o guardar solo los resultados de la ejecución de la tarea. Al hacerlo, reducirá la cantidad de eventos en la base de datos, aumentará la velocidad de ejecución de los escenarios asociados con el análisis de la tabla de eventos en la base de datos y disminuirá el riesgo de que una gran cantidad de eventos sobrescriban eventos críticos.

# Configurar el período máximo de almacenamiento para la información sobre las vulnerabilidades reparadas

Para definir el tiempo por el que la base de datos conservará información sobre las vulnerabilidades reparadas en los dispositivos administrados:

1. Haga clic con el botón derecho en el Servidor de administración y luego seleccione **Propiedades**.

   Se abre la ventana Propiedades del Servidor de administración.

2. En el espacio de trabajo de la sección **Repositorio de eventos**, especifique el período máximo de almacenamiento de la información sobre las vulnerabilidades reparadas en la base de datos.

   De forma predeterminada, el período de almacenamiento es de 90 días.

3. Haga clic en **Aceptar**.

El período de almacenamiento para la información sobre las vulnerabilidades reparadas queda limitado al número de días especificado. Después de eso, la tarea de mantenimiento del Servidor de administración eliminará la información desactualizada de la base de datos.

# Administración de tareas

Kaspersky Security Center administra las aplicaciones instaladas en dispositivos mediante la creación y ejecución de varias tareas. Las tareas son el medio que se utiliza para instalar, iniciar y detener aplicaciones, analizar archivos, actualizar bases de datos y módulos de software y realizar otras acciones en las aplicaciones.

Las tareas se subdividen en los siguientes tipos:

- *Tareas de grupo*. Tareas que se realizan en dispositivos del grupo de administración seleccionado.
- *Tareas del Servidor de administración*. Tareas que se realizan en el Servidor de administración.
- *Tareas para dispositivos específicos*. Tareas que se realizan en dispositivos seleccionados, sin importar si están o no incluidos en algún grupo de administración.
- *Tareas locales*. Tareas que se realizan en un dispositivo específico.

Una tarea de la aplicación solo se puede crear si el complemento de administración para esa aplicación está instalado en la estación de trabajo del administrador.

Puede compilar una lista de dispositivos (hasta 1000) para la que se creará una tarea, mediante uno de los métodos siguientes:

- Al seleccionar dispositivos de la red detectados por el Servidor de administración.
- Al especificar una lista de dispositivos manualmente. Para indicar la dirección de cada dispositivo, puede utilizar una dirección IP (o un intervalo IP), un nombre NetBIOS o un nombre DNS.
- Importar una lista de dispositivos desde un archivo .txt que contenga las direcciones de los dispositivos que se agregarán (cada dirección debe colocarse en una línea individual).

  Si importa una lista de dispositivos desde un archivo o crea una manualmente, y se identifican los dispositivos por sus nombres, la lista debe incluir solamente dispositivos para los que ya se ha ingresado información a la base de datos del Servidor de administración durante la conexión de dichos dispositivos o durante el descubrimiento de dispositivos.

Para cada aplicación puede crear cualquier número de tareas de grupo, tareas para dispositivos específicos o tareas locales.

El intercambio de información acerca de las tareas entre una aplicación instalada en un dispositivo y la base de datos de Kaspersky Security Center se lleva a cabo cuando se conecta el Agente de red al Servidor de administración.

Puede copiar, importar, exportar y eliminar tareas, consultar el progreso de su ejecución y modificar su configuración.

Las tareas se inician en un dispositivo solo si la aplicación para la que se creó está en ejecución. Cuando la aplicación no está en ejecución, se anulan todas las tareas en curso.

Los resultados de tareas completadas se guardan en los registros de eventos de Microsoft Windows y Kaspersky Security Center, tanto centralmente en el Servidor de administración como de forma local en cada dispositivo.

No incluya datos privados en la configuración de las tareas. Por ejemplo, evite especificar la contraseña del administrador del dominio.

### Detalles de la administración de tareas para aplicaciones multiinquilino.

Una tarea de grupo para una aplicación multiinquilino se aplica a la aplicación en función de la jerarquía de los Servidores de administración y los dispositivos cliente. El Servidor de administración virtual desde el que se crea la tarea debe estar en el mismo grupo de administración o en un nivel inferior al del dispositivo cliente en el que está instalada la aplicación.

En los eventos que corresponden a los resultados de la ejecución de la tarea, al administrador del proveedor de servicios se le muestra la información sobre el dispositivo en el que se ejecutó la tarea. Por el contrario, a la administración de un inquilino se le muestra el **Nodo de multiinquilino**.

## Crear una tarea

En la Consola de administración, puede crear tareas directamente en la carpeta del grupo de administración para el que crea la tarea de grupo o en el espacio de trabajo de la carpeta **Tareas**.

*Para crear una tarea de grupo en la carpeta de un grupo de administración:*

1. En el árbol de consola, seleccione el grupo de administración para el que desee crear una tarea.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Tareas**.
3. Ejecute la creación de la tarea con un clic en el botón **Crear una tarea**.

   Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente.

*Para crear una tarea grupal en el espacio de trabajo de la carpeta **Tareas**:*

1. En el árbol de la consola, seleccione la carpeta **Tareas**.
2. Haga clic en el botón **Finalizar** para comenzar a crear la tarea.

   Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente.

No incluya datos privados en la configuración de las tareas. Por ejemplo, evite especificar la contraseña del administrador del dominio.

## Crear una tarea del Servidor de administración

El Servidor de administración realiza las siguientes tareas:

- Entregar informes
- Descargar actualizaciones al repositorio del Servidor de administración
- Copia de seguridad de los datos del Servidor de administración
- Mantenimiento del Servidor de administración
- Sincronización con Windows Update
- Crear un paquete de instalación con la imagen del SO de un dispositivo de referencia
- Instalar aplicación de forma remota
- Desinstalar aplicación de forma remota
- Distribuir paquete de instalación
- Instalar aplicación en Servidores de administración secundarios de forma remota

En un Servidor de administración virtual, solo se encuentran disponibles la tarea de entrega automática de informes y la tarea de creación de paquetes de instalación a partir de la imagen del SO del dispositivo de referencia. El repositorio del Servidor de administración virtual muestra las actualizaciones descargadas al Servidor de administración principal. La copia de seguridad de los datos del Servidor de administración virtual se realiza junto con la copia de seguridad de los datos del Servidor de administración principal.

*Para crear la tarea del Servidor de administración:*

1. En el árbol de la consola, seleccione la carpeta **Tareas**.
2. Realice una de las siguientes acciones para comenzar a crear la tarea:
   - Seleccione **Nuevo** → **Tarea** en el menú contextual de la carpeta **Tareas** en el árbol de la consola.
   - Haga clic en el botón **Crear una tarea** en el espacio de trabajo de la carpeta **Tareas**.

Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente.

Las tareas Descargar actualizaciones en el repositorio del Servidor de administración, Realizar la sincronización con Windows Update, Mantenimiento del Servidor de administración y *Copia de seguridad de los datos del Servidor de administración* se pueden crear una sola vez. Si las tareas *Descargar actualizaciones en el repositorio del Servidor de administración*, *Mantenimiento del Servidor de administración*, *Copia de seguridad de los datos del Servidor de administración* y *Realizar la sincronización con Windows Update* ya se crearon para el Servidor de administración, estas no aparecen en la ventana de la selección del tipo de tarea del Asistente para crear nueva tarea.

## Crear una tarea para dispositivos específicos

En Kaspersky Security Center puede crear tareas para dispositivos específicos. Los dispositivos que se encuentran en un conjunto se pueden incluir en distintos grupos de administración o estar fuera de todos los grupos de administración. Kaspersky Security Center puede realizar las siguientes tareas principales para dispositivos específicos:

- Instalar aplicación de forma remota
- Enviar mensaje a usuario
- Cambiar Servidor de administración
- Administrar dispositivos
- Verificación de actualizaciones
- Distribuir paquetes de instalación
- Instalar aplicación en Servidores de administración secundarios de forma remota
- Desinstalar aplicación de forma remota

*Para crear una tarea para dispositivos específicos:*

1. En el árbol de la consola, seleccione la carpeta **Tareas**.
2. Realice una de las siguientes acciones para comenzar a crear la tarea:
   - Seleccione **Nuevo** → **Tarea** en el menú contextual de la carpeta **Tareas** en el árbol de la consola.
   - Haga clic en el botón **Crear una tarea** en el espacio de trabajo de la carpeta **Tareas**.

Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente.

## Crear una tarea local

*Para crear una tarea local para un dispositivo:*

1. Seleccione la pestaña **Dispositivos** en el espacio de trabajo del grupo que incluye el dispositivo.
2. En la lista de dispositivos de la pestaña **Dispositivos** seleccione el dispositivo para el que se debe crear una tarea local.
3. Comience a crear la tarea para el dispositivo seleccionado mediante una de las siguientes formas:
   - Haga clic en el botón **Realizar acción** y seleccione **Crear una tarea** en la lista desplegable.
   - Haga clic en el enlace **Crear una tarea** en el espacio de trabajo del dispositivo.
   - Use las propiedades del dispositivo, de la forma siguiente:
     a. En el menú contextual del dispositivo, seleccione **Propiedades**.
     b. En la ventana de propiedades de dispositivo que se abre, seleccione la sección **Tareas** y haga clic en **Agregar**.

Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente.

Las instrucciones detalladas sobre cómo crear y configurar tareas locales se proporcionan en las guías de las aplicaciones Kaspersky respectivas.

## Mostrar una tarea de grupo heredada en el espacio de trabajo de un grupo anidado

*Para habilitar la visualización de tareas heredadas de un grupo anidado en el espacio de trabajo:*

1. Seleccione la pestaña **Tareas** en el espacio de trabajo de un grupo anidado.
2. En el espacio de trabajo de la pestaña **Tareas**, haga clic en el botón **Mostrar tareas heredadas**.

Las tareas heredadas se muestran en la lista de tareas con uno de los siguientes iconos:

-  — Si se han heredado de un grupo creado en el Servidor de administración principal.
-  —Si se heredaron de un grupo de nivel superior.

Si está habilitado el modo de herencia, las tareas heredadas solo se pueden modificar en el grupo en que se crearon. Las tareas heredadas no se pueden modificar en el grupo que hereda las tareas.

## Encender dispositivos automáticamente antes de iniciar una tarea

Kaspersky Security Center no puede ejecutar tareas en dispositivos que se encuentran apagados. Por este motivo, puede hacer que Kaspersky Security Center utilice la función "Wake-on-LAN" antes de iniciar una tarea para encender automáticamente los dispositivos apagados.

*Para que los dispositivos apagados se enciendan automáticamente antes de que comience una tarea:*

1. En la ventana de propiedades de la tarea, seleccione la sección **Programación**.
2. Haga clic en el vínculo **Avanzado** para configurar las acciones que se realizarán con los dispositivos.
3. En la ventana que se abre, llamada **Avanzado**, marque la casilla **Encender dispositivos mediante la función Wake-on-LAN antes de iniciar la tarea (min)** e introduzca un número de minutos.

Como resultado, cuando falte el número de minutos indicado para que se inicie la tarea, Kaspersky Security Center usará la función "Wake-on-LAN" para encender los dispositivos y hacer que estos carguen su sistema operativo. Cuando se complete la tarea, los dispositivos en los que nadie haya iniciado sesión se apagarán automáticamente. Tenga en cuenta que Kaspersky Security Center únicamente apagará aquellos dispositivos que se hayan encendido a través de la función "Wake-on-LAN".

Para que Kaspersky Security Center pueda iniciar el sistema operativo de un dispositivo automáticamente, el dispositivo debe ser compatible con el estándar "Wake-on-LAN" (también denominado "WoL").

## Apagar el dispositivo automáticamente una vez que se haya completado la tarea

Kaspersky Security Center permite configurar una tarea de tal manera que los dispositivos a los que se distribuye se apaguen automáticamente una vez que finaliza la tarea.

*Para apagar el dispositivo automáticamente una vez que se haya completado la tarea:*

1. En la ventana de propiedades de la tarea, escoja la sección **Programación**.
2. Haga clic en el enlace **Avanzado** para abrir la ventana para configurar acciones en dispositivos.
3. En la ventana **Avanzado** que se abre, seleccione la casilla de verificación **Apagar dispositivos cuando se complete la tarea**.

## Limitar el tiempo de ejecución de la tarea

*Para limitar el tiempo durante el cual una tarea se ejecuta en dispositivos:*

1. En la ventana de propiedades de la tarea, escoja la sección **Programación**.
2. Abra la ventana correspondiente a la configuración de acciones en dispositivos cliente, haciendo clic en el enlace **Avanzado**.
3. En la ventana **Avanzado** que se abre, seleccione la casilla **Detener la tarea si tarda más de (min)** y especifique el intervalo de tiempo en minutos.

Si la tarea no se ha completado en el dispositivo al caducar el intervalo de tiempo especificado, Kaspersky Security Center detiene la tarea automáticamente.

## Exportar una tarea

Puede exportar tareas de grupo y tareas para dispositivos específicos a un archivo. Las tareas del Servidor de administración no se exportarán.

*Para exportar una tarea:*

1. En el menú contextual de la tarea, seleccione **Todas las tareas** → **Exportar**.
2. En la ventana **Guardar como** que se abre, especifique la ruta del nombre de archivo.
3. Haga clic en el botón **Guardar**.

Los permisos de los usuarios locales no se exportan.

## Importar una tarea

Puede importar tareas de grupo y tareas para dispositivos específicos. Las tareas del Servidor de administración no se importarán.

*Para importar una tarea:*

1. Seleccione la lista a la que se debe importar la tarea:
   - Si desea importar la tarea a la lista de tareas de grupo, en el espacio de trabajo del grupo de administración relevante seleccione la pestaña **Tareas**.
   - Si desea importar una tarea en la lista de tareas para dispositivos específicos, seleccione la carpeta **Tareas** del árbol de consola.
2. Seleccione una de las siguientes opciones para importar la tarea:
   - En el menú contextual de la lista de tareas, seleccione **Todas las tareas → Importar**.
   - Haga clic en el enlace **Importar tarea desde archivo** en el bloque de administración de la lista de tareas.
3. En la ventana que se abrirá, especifique la ruta al archivo desde el cual desea importar una tarea.
4. Haga clic en el botón **Abrir**.

   Se muestra la tarea en la lista de tareas.

Si la tarea importada tiene el mismo nombre que una tarea existente, el nombre de la tarea importada se complementará con un índice secuencial en formato **(<siguiente número secuencial>)**, por ejemplo **(1)** o **(2)**.

## Convertir tareas

Puede usar Kaspersky Security Center para convertir tareas de versiones anteriores de aplicaciones Kaspersky en tareas de versiones actualizadas de las aplicaciones.

La conversión está disponible para tareas de las siguientes aplicaciones:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4
- Kaspersky Endpoint Security 8 para Windows
- Kaspersky Endpoint Security 10 para Windows

*Para convertir tareas:*

1. En el árbol de consola seleccione el Servidor de administración para el que desea convertir tareas.
2. En el menú contextual del Servidor de administración, seleccione **Todas las tareas → Asistente de conversión por lotes de directivas y tareas**.

   Se inicia el Asistente de conversión por lotes de directivas y tareas. Siga las instrucciones del asistente.

Luego de que finalice la operación del asistente, se crearán nuevas tareas que utilizan la configuración de tareas de versiones anteriores de las aplicaciones.

## Iniciar y detener una tarea manualmente

Puede iniciar y detener tareas manualmente usando alguno de los métodos siguientes: desde el menú contextual de la tarea o en la ventana Propiedades del dispositivo cliente al que se asignó esta tarea.

> Solo los usuarios incluidos en el grupo **KLAdmins** tienen permiso para iniciar tareas de grupo desde el menú contextual del dispositivo.

*Para iniciar o detener una tarea desde el menú contextual o la ventana de propiedades de la tarea, haga lo siguiente:*

1. En la lista de tareas, seleccione una tarea.
2. Inicie o detenga la tarea de una de las siguientes formas:
   - Seleccione **Iniciar** o **Detener** en el menú contextual de la tarea.
   - Haga clic en **Iniciar** o **Detener** en la sección **General** de la ventana de propiedades de la tarea.

*Para iniciar o detener una tarea desde el menú contextual o la ventana de propiedades del dispositivo cliente, haga lo siguiente:*

1. En la lista de dispositivos, seleccione el dispositivo.
2. Inicie o detenga la tarea de una de las siguientes formas:
   - Seleccione **Todas las tareas** → **Ejecutar una tarea** en el menú contextual del dispositivo. Seleccione la tarea correspondiente de la lista de tareas.

     La lista de dispositivos a los que está asignada la tarea será reemplazada por el dispositivo que ha seleccionado. Se inicia la tarea.
   - Haga clic en el botón Iniciar (  ) o en el botón Detener (  ) en la sección **Tareas** de la ventana de propiedades del dispositivo.

## Pausar y reanudar una tarea manualmente

*Para pausar o reanudar la ejecución de una tarea manualmente:*

1. En la lista de tareas, seleccione una tarea.
2. Pause o reanude la tarea mediante uno de los siguientes métodos:
   - Seleccionando **Pausar** o **Reanudar** en el menú contextual de la tarea.
   - Al seleccionar la sección **General** en la ventana de propiedades de la tarea y al hacer clic en **Pausar** o **Reanudar**.

## Supervisar la ejecución de tareas

*Para supervisar la ejecución de tareas,*

en la ventana de propiedades de la tarea, seleccione la sección **General**.

En la parte media de la sección **General**, se muestra el estado de la tarea actual.

## Ver resultados de la ejecución de tareas almacenados en el Servidor de administración

Kaspersky Security Center le permite ver resultados de la ejecución para tareas de grupos, tareas para dispositivos específicos y tareas del Servidor de administración.

*Para ver los resultados de la tarea:*

1. En la ventana de propiedades de la tarea, seleccione la sección **General**.
2. Haga clic en el enlace **Resultados** para abrir la ventana **Resultados de la tarea**.

*Para ver los resultados de la tarea de un Servidor de administración secundario:*

1. En la ventana de propiedades de la tarea, seleccione la sección **General**.
2. Haga clic en el vínculo **Resultados** para abrir la ventana **Resultados de la tarea**.
3. Haga clic en **Estadísticas de los servidores secundarios**.
4. Seleccione el servidor secundario para el que desea mostrar la ventana **Resultados de la tarea**.

## Configurar el filtrado de información sobre resultados de la ejecución de tareas

Kaspersky Security Center permite filtrar información sobre resultados de ejecución para tareas de grupos, tareas para dispositivos específicos y tareas del Servidor de administración. El filtrado no está disponible para tareas locales.

*Para configurar el filtrado de información sobre resultados de ejecución de tareas:*

1. En la ventana de propiedades de la tarea, seleccione la sección **General**.
2. Haga clic en el enlace **Resultados** para abrir la ventana **Resultados de la tarea**.

   La tabla de la parte superior contiene una lista de todos los dispositivos para los que se asignó la tarea. La tabla de la parte inferior muestra los resultados de la tarea realizada en el dispositivo seleccionado.

3. Haga clic con el botón derecho del mouse para abrir el menú contextual y seleccione **Filtro**.

4. En el ventana **Establecer filtro** que se abre, configure el filtro en las secciones **Eventos**, **Dispositivos** y **Hora**. Haga clic en **Aceptar**.

La ventana **Resultados de la tarea** muestra información que coincide con la configuración especificada en el filtro.

## Modificar una tarea. Reversión de cambios

*Para modificar una tarea:*

1. En el árbol de la consola, seleccione la carpeta **Tareas**.

2. En el espacio de trabajo de la carpeta **Tareas**, seleccione una tarea y vaya a la ventana de propiedades de la tarea usando el menú contextual.

3. Haga los cambios relevantes.

> En la sección **Exclusiones del alcance de la tarea**, puede configurar la lista de subgrupos a los que no se aplica la tarea.

4. Haga clic en **Aplicar**.

Los cambios hechos a la tarea se guardarán en la ventana Propiedades de la tarea, en la sección **Historial de revisiones**.

Puede deshacer los cambios hechos en la tarea, si es necesario.

*Para deshacer cambios hechos en una tarea:*

1. En el árbol de la consola, seleccione la carpeta **Tareas**.

2. Seleccione la tarea donde se deben deshacer los cambios y vaya a la ventana de propiedades de la tarea usando el menú contextual.

3. En la ventana de propiedades de la tarea, seleccione la sección **Historial de revisiones**.

4. En la lista de revisiones de la tarea, seleccione el número de la revisión en la cual necesita deshacer cambios.

5. Haga clic en el botón **Avanzado** y seleccione el valor **Revertir** en la lista desplegable.

# Comparación de tareas

Puede comparar tareas del mismo tipo: por ejemplo, puede comparar dos tareas de análisis antimalware, pero no puede comparar una tarea de análisis antimalware y una tarea de instalación de actualizaciones. Después de la comparación, tiene un informe que muestra con qué configuración de las tareas coinciden y qué configuración diferencian. Puede imprimir el informe de la comparación de la tarea o guardarlo como un archivo. Puede necesitar la comparación de la tarea cuando las unidades diferentes en un plazo de una empresa se asignan varias tareas del mismo tipo. Por ejemplo, los empleados del departamento de contabilidad tienen una tarea de análisis antimalware solo en los discos locales de sus dispositivos, mientras que los empleados del departamento de ventas se comunican con clientes y, por tanto, tienen una tarea de análisis tanto de discos locales como de correo electrónico. Para ver rápidamente dichas diferencias, no es necesario ver todos los parámetros de la tarea, porque basta con realizar una comparación de tareas.

Solo las tareas del mismo tipo se pueden comparar.

Las tareas solo se pueden comparar en pares.

Puede comparar tareas de una de estas formas: seleccionar una tarea y compararla con otra, o comparar dos tareas desde la lista de tareas.

*Seleccionar una tarea y compararla con otra:*

1. En el árbol de la consola, seleccione la carpeta **Tareas**.
2. En el espacio de trabajo de la carpeta **Tareas**, seleccione la tarea que desea comparar con otra.
3. En el menú contextual de la tarea, seleccione **Todas las tareas** → **Comparar con otra tarea**.
4. En la ventana **Elija una tarea**, seleccione la tarea para la comparación.
5. Haga clic en **Aceptar**.

   Un informe en el formato de HTML que compara las dos tareas se muestra.

*Para comparar dos tareas de la lista de tareas:*

1. En el árbol de la consola, seleccione la carpeta **Tareas**.
2. En la carpeta **Tareas**, en la lista de tareas, presione la tecla **`Mayús`** o **`Ctrl`** para seleccionar dos tareas del mismo tipo.
3. En el menú contextual, seleccione **Comparar**.

   Se muestra un informe en formato de HTML que compara las tareas seleccionadas.

Cuando se comparan las tareas, si las contraseñas difieren, se muestran asteriscos (******) en el informe de comparación de la tarea.

Si se modificó la contraseña en las propiedades de la tarea, se muestran asteriscos (******) en el informe de comparación de la revisión (******).

## Cuentas para iniciar tareas

Puede especificar una cuenta según la cual se ejecutará la tarea.

Por ejemplo, para realizar una tarea de análisis a pedido, necesita los permisos de acceso al objeto que se analiza; y para realizar una tarea de actualización, necesita los derechos del usuario de servidor proxy autorizado. La capacidad de especificar una cuenta para la ejecución de la tarea le permite evitar los problemas con las tareas de análisis a pedido y las tareas de actualización cuando el usuario que ejecuta una tarea no tiene los permisos de acceso requeridos.

Durante la ejecución de las tareas de instalación o desinstalación remotas, la cuenta especificada se utiliza para descargar a los dispositivos cliente los archivos requeridos para instalar o desinstalar una aplicación en caso de que no se haya instalado o no esté disponible el Agente de red. Cuando el Agente de red está instalado y disponible, la cuenta se usa si, de acuerdo con la configuración de tareas, el envío de archivos se realiza mediante las utilidades de Microsoft Windows desde la carpeta compartida únicamente. En este caso la cuenta debe tener los siguientes permisos en el dispositivo:

- Permiso para iniciar aplicaciones de forma remota.
- Permisos para usar el recurso Admin$.
- Permiso para *iniciar sesión como servicio*.

Si se envían los archivos a los dispositivos por medio del Agente de red, la cuenta no se usará. Todas las operaciones de copia e instalación de archivos son realizadas por el **Agente de red** (**Cuenta del sistema local**).

## Exportar el historial de ejecución de tareas

Si encuentra algún problema con una tarea, es posible que necesite investigar las razones subyacentes. Para ello, puede exportar y analizar más a fondo el historial de ejecución de tareas.

*Para exportar el historial de ejecución de tareas:*

1. Cree un archivo TXT vacío en un directorio de su dispositivo.

   El historial de ejecución de tareas se exportará a este archivo.

2. Abra la ventana de resultados de la tarea.

3. En la parte superior de la ventana de resultados de la tarea, seleccione el dispositivo que está experimentando problemas.

4. En la parte inferior de la ventana de resultados de la tarea, donde se muestra el historial de ejecución del dispositivo seleccionado, seleccione uno o varios eventos.

   Para seleccionar varios eventos, utilice la clave **`Shift`** o **`Ctrl`**.

5. Haga clic con el botón derecho del mouse para abrir el menú contextual y seleccione **Exportar**.

   Se inicia el Asistente de exportación de eventos.

6. En el paso **Archivo al que exportar** del asistente, haga clic en el botón **Examinar** y luego seleccione el archivo TXT que ha creado para exportar el historial de ejecución de tareas.

   Si desea exportar solo la selección de eventos, habilite la opción **Exportar solo los eventos seleccionados**.

   Si desea exportar todo el historial de ejecución de tareas (todos los eventos), la opción **Exportar solo los eventos seleccionados** debe estar deshabilitada.

7. Haga clic en el botón **Siguiente**.

8. En el paso **Formato de exportación** del asistente, active una de las siguientes opciones:

   - **Exportar como texto Unicode separado por tabulaciones**

     Active esta opción si los datos exportados incluyen caracteres especiales y símbolos de varios idiomas y necesita asegurarse de que todos los caracteres se conserven con precisión cuando el archivo TXT con los datos exportados se abra en diferentes aplicaciones.

   - **Exportar como texto separado por tabulaciones**

     Active esta opción si desea mantener la compatibilidad con sistemas o aplicaciones más antiguos que pueden no ser compatibles con Unicode.

9. Haga clic en el botón **Siguiente** para finalizar el asistente.

El historial de ejecución de tareas se exporta al archivo TXT seleccionado.

## Asistente para cambiar contraseñas de tareas

Para una tarea no local, puede especificar una cuenta en la que se debe ejecutar la tarea. La cuenta puede definirse al momento de crear la tarea; si la tarea ya existe, puede definirse en sus propiedades. Si la cuenta especificada se usa de acuerdo con las instrucciones de seguridad de la organización, estas instrucciones pueden requerir cambiar la contraseña de la cuenta de vez en cuando. Cuando la contraseña de la cuenta caduca y usted configura una nueva, las tareas no se iniciarán hasta que especifique la nueva contraseña válida en las propiedades de la tarea.

El Asistente para cambiar contraseñas de tareas permite reemplazar automáticamente la contraseña antigua por una nueva en todas las tareas en las que se utiliza la cuenta especificada. Alternativamente, puede hacerlo manualmente en las propiedades de cada tarea.

*Para iniciar el Asistente para cambiar contraseñas de tareas:*

1. En el árbol de consola, seleccione el nodo **Tareas**.

2. En el menú contextual del nodo, seleccione **Asistente para cambiar contraseñas de tareas**.

Siga las instrucciones del asistente.

### Paso 1. Especificar credenciales

En los campos **Cuenta** y **Contraseña**, especifique nuevas credenciales que sean válidas actualmente en su sistema (por ejemplo, en Active Directory). Cuando cambia al siguiente paso del asistente, Kaspersky Security Center verifica si el nombre de cuenta especificado coincide con el nombre de cuenta en las propiedades de cada tarea no local. Si los nombres de las cuentas coinciden, la contraseña en las propiedades de la tarea se reemplazará automáticamente por la nueva.

Si completa el campo **Contraseña anterior (opcional)**, Kaspersky Security Center reemplaza la contraseña solo para aquellas tareas en las que se encuentran tanto el nombre de la cuenta como la contraseña anterior. El reemplazo se realiza automáticamente. En todos los demás casos, debe elegir una acción para realizar el siguiente paso del Asistente.

### Paso 2. Seleccionar una acción para realizar

Si no ha especificado la contraseña anterior en el primer paso del Asistente o si la contraseña anterior especificada no coincide con las contraseñas en las tareas, debe elegir una acción para las tareas encontradas.

Para cada tarea que tiene el estado *Debe aprobarse*, decida si desea eliminar la contraseña en las propiedades de la tarea o reemplazarla por la nueva. Si elige eliminar la contraseña, la tarea cambia para ejecutarse con la cuenta predeterminada.

### Paso 3. Ver los resultados

En el último paso del Asistente, vea los resultados de cada una de las tareas encontradas. Para finalizar el Asistente, haga clic en el botón **Finalizar**.

# Creación de una jerarquía de grupos de administración subordinados a un Servidor de administración virtual.

Una vez creado el Servidor de administración virtual, tendrá, de manera predeterminada, un grupo de administración denominado **Dispositivos administrados**.

El procedimiento de creación de una jerarquía de grupos de administración subordinados al Servidor de administración virtual es el mismo que el procedimiento de creación de una jerarquía de grupos de administración subordinados al Servidor de administración físico.

No se pueden agregar Servidores de administración secundarios y virtuales a los grupos de administración subordinados a un Servidor de administración virtual. Esto se debe a limitaciones de los Servidores de administración virtuales.

# Directivas y perfiles de directivas

En Kaspersky Security Center Web Console, puede crear directivas para las aplicaciones de Kaspersky. En esta sección se explica qué son, cómo se crean y cómo se modifican las directivas y los perfiles de directivas.

## Jerarquía de directivas, usando perfiles de directivas

En esta sección se proporciona información sobre cómo aplicar directivas a los dispositivos en los grupos de administración. Esta sección también proporciona información sobre los perfiles de directivas.

## Jerarquía de directivas

En Kaspersky Security Center, usa directivas para definir una sola colección de configuración para múltiples dispositivos. Por ejemplo, el alcance de la directiva de la aplicación P definido para el grupo de administración G incluye los dispositivos administrados que tienen la aplicación P instalada y que se han agregado al grupo G o a cualquiera de sus subgrupos, excepto los subgrupos donde la casilla **Heredar del grupo primario** está desmarcada en las propiedades.

Una directiva se diferencia de cualquier parámetro local por los candados (🔒) que aparecen al lado de su configuración. Si una configuración (o un grupo de configuraciones) está bloqueada en las propiedades de la directiva, debe usar, en primer lugar, esta configuración (o grupo de configuraciones) al crear la configuración vigente y, en segundo lugar, debe escribir la configuración o el grupo de configuraciones en la directiva descendente.

La creación de la configuración vigente en un dispositivo se puede describir de la forma siguiente: los valores de toda la configuración que no se hayan bloqueado se toman desde la directiva, a continuación se sobrescriben con los valores de la configuración local, y luego la recolección resultante se sobrescribe con los valores de la configuración bloqueada tomada desde la directiva.

Las directivas de la misma aplicación se afectan mutuamente a través de la jerarquía de grupos de administración: la configuración bloqueada desde la directiva descendente sobrescribe la misma configuración desde la directiva descendente.

Hay una directiva especial para los usuarios fuera de la oficina. Esta directiva entra en vigor en un dispositivo cuando el dispositivo cambia al modo fuera de la oficina. Las directivas fuera de la oficina no afectan a otras directivas a través de la jerarquía de grupos de administración.

## Perfiles de directivas

En muchas circunstancias, puede ser inconveniente aplicar directivas a dispositivos solo mediante la jerarquía de grupos de administración. Puede ser necesario crear varias instancias de una sola directiva que se diferencien en una o dos configuraciones para grupos de administración diferentes, y sincronizar los contenidos de esas directivas en el futuro.

Para ayudarle a evitar tales problemas, Kaspersky Security Center admite *perfiles de directivas*. Un perfil de directiva es un subconjunto nominado de los valores de configuración definidos en una directiva. Este subconjunto se distribuye en dispositivos de destino junto con la directiva, y se complementa bajo una condición específica denominada *Condición de activación del perfil*. Los perfiles solo contienen configuraciones que se diferencian de la directiva "básica" que está activa en el dispositivo cliente (equipo o dispositivo móvil). Al activarse un perfil se modifica la configuración de directiva que se encontraba activa en el dispositivo antes de que se activara el perfil. Dicha configuración tomará los valores que se habían especificado en el perfil.

Las restricciones siguientes se imponen actualmente en los perfiles de directivas:

- Una directiva puede incluir un máximo de 100 perfiles.
- Un perfil de directivas no puede contener otros perfiles.
- Un perfil de directivas no puede contener una configuración de notificaciones.

## Contenido de un perfil

Un perfil de directivas contiene las siguientes partes:

- Perfiles de nombre con nombres idénticos que se afectan mutuamente a través de la jerarquía de grupos de administración con reglas comunes.
- Subconjunto de configuración de la directiva. A diferencia de la directiva, que contiene todas las configuraciones, un perfil solo contiene configuraciones que realmente se requieren (configuraciones bloqueadas).
- La condición de activación es una expresión lógica con propiedades del dispositivo. Un perfil está activo (complementa a la directiva) solo cuando la condiciones de activación del perfil se hace verdadera. En todos los otros casos, el perfil está inactivo y es ignorado. Las propiedades del dispositivo siguientes se pueden incluir en esa expresión lógica:
  - Estado de modo fuera de la oficina.
  - Propiedades del entorno de la red; nombre de la regla activa para conexión con el Agente de red.
  - Presencia o ausencia de etiquetas específicas en el dispositivo.
  - El hecho de que el dispositivo pertenezca a una unidad de Active Directory, sea esta relación de pertenencia explícita (el dispositivo se encuentra en la unidad organizativa especificada) o implícita (el dispositivo está en una unidad organizativa que se encuentra dentro de la unidad especificada, sin importar el nivel de anidamiento).
  - Membrecía del dispositivo en un grupo de seguridad de Active Directory (explícita o implícita).
  - Membrecía del propietario del dispositivo en un grupo de seguridad de Active Directory (explícita o implícita).
- Casilla de deshabilitación del Perfil. Los perfiles deshabilitados siempre se ignoran y sus condiciones de activación respectivas no se verifican.
- Prioridad del Perfil. Las condiciones de activación de perfiles diferentes son independientes, por lo tanto varios perfiles se pueden activar simultáneamente. Si los perfiles activos contienen recolecciones no superpuestas de configuraciones, no se producirá ningún problema. Sin embargo, si dos perfiles activos contienen valores diferentes de la misma configuración, una ambigüedad ocurrirá. Esta ambigüedad se debe evitar a través de prioridades del perfil: El valor de la variable ambigua se tomará desde el perfil que tiene la prioridad más alta (el que se califica más alto en la lista de perfiles).

## Comportamiento de los perfiles cuando las directivas se afectan mutuamente a través de la jerarquía

Los perfiles con el mismo nombre se fusionan según las reglas de fusión de directivas. Los perfiles de una directiva ascendente tienen una prioridad más alta que los perfiles de una directiva descendente. Si la edición de la configuración se prohíbe en la directiva ascendente (está bloqueada), la directiva descendente usa las condiciones de activación del perfil de la ascendente. Si la edición de la configuración está permitida en la directiva ascendente, las condiciones de activación del perfil desde la directiva descendente se utilizan.

Como un perfil de directivas puede contener la propiedad **El dispositivo no tiene conexión** en su condición de activación, los perfiles reemplazan completamente la función de las directivas para los usuarios fuera de la oficina, que ya no se admitirán.

Una directiva para usuarios fuera de la oficina puede contener perfiles, pero sus perfiles solo se pueden activar después de que el dispositivo cambie al modo fuera de la oficina.

### Herencia de configuración de la directiva

Se especifica una directiva para un grupo de administración. La configuración de una directiva puede ser *heredada* (es decir, recibida) por los subgrupos (grupos secundarios) del grupo de administración para el que esa directiva fue creada (el grupo primario). En lo sucesivo, se usará el término *directiva primaria* para hacer referencia a una directiva definida para un grupo primario.

Puede habilitar o deshabilitar dos opciones de herencia: **Heredar configuraciones de la directiva principal** y **Forzar herencia de configuraciones en las directivas secundarias**:

- Si habilita la configuración **Heredar de la directiva principal** para una directiva secundaria y bloquea algunas configuraciones en la directiva principal, no puede cambiar esta configuración para el grupo secundario. Sí podrá, en cambio, modificar cualquier ajuste que no se encuentre bloqueado en la directiva primaria.

- Si deshabilita la **Heredar configuración desde la directiva primaria** para una directiva secundaria, puede cambiar todas las configuraciones en el grupo secundario, incluso si algunas configuraciones están bloqueadas en la directiva principal.

- Si habilita **Forzar herencia de configuraciones en directivas secundarias en el grupo primario**, esto habilita la **Herencia de configuraciones de la directiva principal** para cada directiva secundaria. No podrá deshabilitar esta opción en ninguna directiva secundaria. Los grupos secundarios heredarán forzosamente todos los ajustes de configuración que se encuentren bloqueados en la directiva primaria. Los valores de esos ajustes no se podrán modificar en los grupos secundarios.

- En las directivas para el grupo de **Dispositivos administrados**, **Heredar configuración desde la directiva primaria** no afecta a ninguna configuración, ya que el grupo de **Dispositivos administrados** no tiene ningún grupo ascendente y, por lo tanto, no hereda ninguna directiva.

De forma predeterminada, la opción **Heredar configuraciones de la directiva principal** está habilitada para una nueva directiva.

Si una directiva tiene perfiles, todas las directivas secundarias los heredan.

## Administración de directivas

Las aplicaciones instaladas en los dispositivos cliente se configuran de modo centralizado a través de la definición de directivas.

Las directivas creadas para las aplicaciones de un grupo de administración se muestran en el espacio de trabajo de la pestaña **Directivas**. Delante del nombre de cada directiva, se muestra un icono con su estado.

Después de eliminar o revocar una directiva, la aplicación continúa trabajando con la configuración especificada en la directiva. Posteriormente, esa configuración se puede modificar manualmente.

Una directiva rige de la siguiente manera: si un dispositivo está ejecutando tareas residentes (tareas de protección en tiempo real), estas continúan ejecutándose con los nuevos valores de la configuración. Cualquier tarea periódica (análisis a pedido, actualización de bases de datos de la aplicación) que haya comenzado se seguirá ejecutando con los valores sin modificar. La próxima vez, se ejecutarán con los valores de parámetro nuevos.

Las directivas para aplicaciones multiinquilino se heredan a grupos de administración de nivel inferior así como a grupos de administración de nivel superior: la directiva se propaga a todos los dispositivos cliente en los que está instalada la aplicación.

Si los Servidores de administración tienen una estructura jerárquica, los Servidores secundarios reciben directivas del Servidor de administración principal y las distribuyen a los dispositivos cliente. Cuando está habilitada la herencia, la configuración de la directiva se puede modificar en el Servidor de administración principal. Luego de ello, cualquier cambio realizado a la configuración de la directiva se propaga a las directivas heredadas de los Servidores de administración secundarios.

Si finaliza la conexión entre los Servidores de administración principal y secundario, la directiva en el Servidor secundario seguirá usando la configuración aplicada. La configuración de la directiva modificada en el Servidor de administración principal se distribuye a un Servidor de administración secundario una vez restablecida la conexión.

Si se deshabilita la herencia, la configuración de la directiva se puede modificar en un Servidor de administración secundario, independientemente del Servidor de administración principal.

Si se interrumpe la conexión entre un Servidor de administración y un dispositivo cliente, el dispositivo cliente empezará a trabajar con la directiva fuera de la oficina (si está definida) o la directiva seguirá usando los parámetros aplicados hasta que se restablezca la conexión.

Los resultados de la distribución de directivas en el Servidor de administración secundario se muestran en la ventana de propiedades de la directiva en la consola del Servidor de administración principal.

Los resultados de la distribución de directivas en dispositivos cliente se muestran en la ventana de propiedades de la directiva del Servidor de administración al que están conectados.

No use datos privados en la configuración de directivas. Por ejemplo, evite especificar la contraseña del administrador del dominio.

## Crear una directiva

En la Consola de administración, puede crear directivas directamente en la carpeta del grupo de administración para el que crea la directiva o en el espacio de trabajo de la carpeta **Directivas**.

*Para crear una directiva en la carpeta de un grupo de administración:*

1. En el árbol de consola, seleccione el grupo de administración para el que desea crear una directiva.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Haga clic en el botón **Nueva directiva** para ejecutar el Asistente de nueva directiva.

   El Asistente de nueva directiva se inicia. Siga las instrucciones del asistente.

*Para crear una directiva en el espacio de trabajo de la carpeta **Directivas**:*

1. En el árbol de la consola, seleccione la carpeta **Directivas**.
2. Haga clic en el botón **Nueva directiva** para ejecutar el Asistente de nueva directiva.

El Asistente de nueva directiva se inicia. Siga las instrucciones del asistente.

Puede crear varias directivas para una aplicación desde el grupo; no obstante, solo una directiva puede estar activa por vez. Cuando se crea una nueva directiva activa, la directiva activa anterior pasa a estar inactiva.

Cuando se crea una directiva, puede especificar un conjunto mínimo de parámetros requeridos para el funcionamiento correcto de la aplicación. El resto de los valores se establecen en los valores predeterminados aplicados en la instalación local de la aplicación. Puede modificar la directiva una vez que está creada.

No use datos privados en la configuración de directivas. Por ejemplo, evite especificar la contraseña del administrador del dominio.

La configuración de las aplicaciones Kaspersky modificada luego de aplicar las directivas se describe en detalle en las guías respectivas.

Después de que la directiva se crea, la configuración bloqueada para la edición (marcadas con el bloqueo ) entra en vigor en los dispositivos cliente independientemente de qué configuración se había especificado previamente para la aplicación.

## Mostrar directiva heredada en un subgrupo

*Para habilitar la visualización de directivas heredadas para un grupo de administración heredado:*

1. En el árbol de consola, seleccione el grupo de administración para el que se deben mostrar las directivas heredadas.
2. En el espacio de trabajo del grupo seleccionado, seleccione la pestaña **Directivas**.
3. En el menú contextual de la lista de directivas, seleccione **Ver** → **Directivas heredadas**.

Las directivas heredadas se muestran en la lista de directivas con el siguiente icono:

- —Si se heredaron de un grupo creado en el Servidor de administración principal.
- —Si se heredaron de un grupo de nivel superior.

Cuando está habilitado el modo de herencia de configuración, las directivas heredadas solo están disponibles para modificación en el grupo en que se crearon. La modificación de directivas heredadas no está disponible en el grupo que las hereda.

## Activar una directiva

*Para activar una directiva para el grupo seleccionado:*

1. En el espacio de trabajo del grupo, en la pestaña **Directivas** seleccione la directiva que necesita activar.
2. Para activar la directiva, realice una de las siguientes acciones:
   - En el menú contextual de la directiva, seleccione **Directiva activa**.
   - En la ventana de propiedades de la directiva, abra la sección **General** y seleccione **Directiva activa** en el grupo de configuración **Estado de la directiva**.

La directiva pasa a estar activa para el grupo de administración seleccionado.

Cuando se aplica una directiva a un gran número de dispositivos cliente, tanto la carga en el Servidor de administración como el tráfico de red aumentan significativamente durante un tiempo.

## Activar una directiva automáticamente ante un brote de virus

*Para que una directiva se active automáticamente al ocurrir un evento Brote de virus, haga lo siguiente:*

1. En la ventana de propiedades del Servidor de administración, abra la sección **Brote de virus**.
2. Abra la ventana **Activación de directiva** haciendo clic en el enlace **Configurar las directivas que se activarán ante un brote de virus** y agregue la directiva a la lista seleccionada de directivas que se activan cuando se detecta un brote de virus.

Si se activa una directiva en el evento *Brote de virus*, la única forma de volver a la directiva anterior es mediante el modo manual.

## Aplicación de una directiva fuera de la oficina

La directiva fuera de la oficina entra en vigencia en un dispositivo en el caso de que dicho dispositivo se desconecte de la red corporativa.

*Para aplicar la directiva fuera de la oficina, haga lo siguiente:*

En la ventana de propiedades de la directiva, abra la sección **General** y en el grupo de configuración **Estado de la directiva** seleccione **Directiva para fuera de la oficina**.

La directiva fuera de la oficina se aplicará en los dispositivos que se desconecten de la red corporativa.

## Modificación de una directiva. Reversión de cambios

*Para modificar una directiva:*

1. En el árbol de la consola, seleccione la carpeta **Directivas**.
2. En el espacio de trabajo de la carpeta **Directivas**, seleccione una directiva y vaya a la ventana Propiedades de la directiva usando el menú contextual.
3. Haga los cambios relevantes.
4. Haga clic en **Aplicar**.

   Los cambios hechos a la directiva se guardarán en las propiedades de la directiva, en la sección **Historial de revisiones**.

Puede deshacer los cambios hechos en la directiva, si es necesario.

*Para deshacer cambios hechos en la directiva:*

1. En el árbol de la consola, seleccione la carpeta **Directivas**.
2. Seleccione la directiva donde se deben deshacer los cambios y vaya a la ventana de propiedades de la directiva usando el menú contextual.
3. En la ventana de propiedades de la directiva, seleccione la sección **Historial de revisiones**.
4. En la lista de revisiones de la directiva, seleccione el número de la revisión en la cual necesita deshacer cambios.
5. Haga clic en el botón **Avanzado** y seleccione el valor **Revertir** en la lista desplegable.

## Comparación de directivas

Puede comparar dos directivas para una aplicación administrada sola. Después de la comparación, tiene un informe que muestra qué configuración de la directiva coincide y qué configuración difiere. Debería comparar, por ejemplo, directivas si los administradores diferentes en sus oficinas respectivas han creado directivas varias para una aplicación administrada sola, o si una directiva de alto nivel sola ha sido heredada por todas las oficinas locales y se ha modificado para cada oficina. Puede comparar directivas de una de estas formas: al seleccionar una directiva y al compararla con otra, o al comparar dos directivas desde la lista de directivas.

Solo puede comparar directivas que tengan revisiones actuales en el historial de revisiones.

*Comparar una directiva otra:*

1. En el árbol de la consola, seleccione la carpeta **Directivas**.
2. En el espacio de trabajo de la carpeta **Directivas**, seleccione la directiva que desea comparar con otra.
3. En el menú contextual de la directiva, seleccione **Comparar directiva con otra directiva**.

4. En la ventana **Seleccionar directiva**, seleccione la directiva con la cual su directiva se debe comparar.

5. Haga clic en **Aceptar**.

   Un informe en el formato de HTML se muestra para la comparación de las dos directivas para la misma aplicación.

*Comparar dos directivas desde la lista de directivas:*

1. En la carpeta **Directivas**, en la lista de directivas, use la tecla **Mayús** o **Ctrl** para seleccionar dos directivas para una misma aplicación administrada.

2. En el menú contextual, seleccione **Comparar**.

   Un informe en el formato de HTML se muestra para la comparación de las dos directivas para la misma aplicación.

   El informe sobre la comparación de la configuración de la directiva para Kaspersky Endpoint Security para Windows también proporciona detalles de la comparación de los perfiles de las directivas. Puede minimizar los resultados de la comparación del perfil de directiva. Para minimizar la sección, haga clic en el ícono de flecha ( ) al lado del nombre de la sección.

## Ver el gráfico de distribución de una directiva

En Kaspersky Security Center, puede ver los resultados de la aplicación de la directiva sobre cada dispositivo.

*Para ver el estado de distribución de una directiva en cada dispositivo:*

1. En el espacio de trabajo del grupo, en la pestaña **Directivas**, seleccione la directiva cuyo estado de distribución desee consultar.

   En el gráfico del panel derecho, se muestra la descripción general de la aplicación de la directiva.

2. Haga clic en **Detalles**.

   Se abre la ventana **Resultados de la aplicación de la directiva**.

   Puede exportar los resultados de la aplicación de la directiva a un archivo CSV o TXT.

## Eliminar una directiva

*Para eliminar una directiva:*

1. En el espacio de trabajo de un grupo de administración, en la pestaña **Directivas**, seleccione la directiva que desea eliminar.

2. Elimine la directiva de una de las siguientes formas:

   - Seleccione **Eliminar** en el menú contextual de la directiva.

   - Haga clic en el enlace **Eliminar directiva** en el cuadro de información de la directiva seleccionada.

## Copiar una directiva

*Para copiar una directiva:*

1. En el espacio de trabajo del grupo requerido, en la pestaña **Directivas**, seleccione una directiva.
2. En el menú contextual de la directiva, seleccione **Copiar**.
3. En el árbol de consola, seleccione un grupo para el cual desea agregar la directiva.

   Puede agregar la directiva al grupo desde el cual se copió.
4. En el menú contextual de la lista de directivas para el grupo seleccionado, en la pestaña **Directivas** seleccione **Pegar**.

La directiva se copia con toda su configuración y se implementa en los dispositivos del grupo en el que se la copió. Si pega la directiva en el mismo grupo desde el cual se la copió, el índice **(<siguiente número de la secuencia>)** se agrega automáticamente al nombre de la directiva; por ejemplo, **(1)**, **(2)**.

Una directiva activa pasa a estar inactiva mientras se copia. Si es necesario, se puede activar.

## Exportación de una directiva

*Para exportar una directiva:*

1. Exporte una directiva de una de las siguientes formas:
   - Seleccione **Todas las tareas** → **Exportar** en el menú contextual de la directiva.
   - Haga clic en el vínculo **Exportar directiva a archivo** en el cuadro de información de la directiva seleccionada.
2. En la ventana **Guardar como** que se abre, especifique el nombre de archivo de la directiva y la ruta. Haga clic en el botón **Guardar**.

## Importación de una directiva

*Para importar una directiva:*

1. En el espacio de trabajo del grupo relevante, en la pestaña **Directivas**, seleccione uno de los siguientes métodos para importar directivas:
   - Seleccione **Todas las tareas** → **Importar** en el menú contextual de la lista de directivas.
   - Haga clic en el botón **Importar directiva desde archivo** en el bloque administrativo para la lista de directiva.
2. En la ventana que se abrirá, especifique la ruta al archivo desde el cual desea importar una directiva. Haga clic en el botón **Abrir**.

La directiva importada aparecerá en la lista de directivas. También se importarán la configuración y los perfiles de la directiva. La directiva importada tendrá estado inactivo independientemente del estado que se haya seleccionado al exportarla. Puede cambiar el estado en las propiedades de la directiva.

Si la directiva importada tiene el mismo nombre que una directiva existente, el nombre de la directiva importada se complementará con un índice secuencial en formato **(<siguiente número secuencial>)**, por ejemplo **(1)** o **(2)**.

## Convertir directivas

Kaspersky Security Center puede convertir las directivas de versiones anteriores de aplicaciones de Kaspersky administradas en directivas de versiones actualizadas de las mismas aplicaciones. Las directivas convertidas mantienen los ajustes definidos por el administrador antes de la actualización e incorporan, también, los nuevos ajustes disponibles en las versiones actualizadas de las aplicaciones. Si una directiva se convierte a una versión actualizada de una aplicación administrada de Kaspersky, no podrá abrir la directiva en un Servidor de administración que tenga instalada una versión anterior del complemento de la aplicación. Los complementos de administración para las aplicaciones de Kaspersky determinan si es posible o no convertir las directivas de las aplicaciones correspondientes. Si desea obtener instrucciones para convertir las directivas de cada aplicación de Kaspersky admitida, consulte la ayuda correspondiente (puede usar los vínculos de la siguiente lista):

- **Aplicaciones de Kaspersky para estaciones de trabajo:**
  - Kaspersky Endpoint Security para Windows
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Linux Elbrus Edition
  - Kaspersky Endpoint Security for Mac
  - Kaspersky Endpoint Agent
  - Kaspersky Embedded Systems Security para Windows
- **Kaspersky Industrial CyberSecurity:**
  - Kaspersky Industrial CyberSecurity for Nodes
  - Kaspersky Industrial CyberSecurity for Linux Nodes
  - Kaspersky Industrial CyberSecurity for Networks (no se admite el despliegue centralizado)
- **Aplicaciones de Kaspersky para dispositivos móviles:**
  - Kaspersky Endpoint Security para Android
  - Kaspersky Security for iOS

- **Aplicaciones de Kaspersky para servidores de archivos:**
  - Kaspersky Security for Windows Server
  - Kaspersky Endpoint Security para Windows
  - Kaspersky Endpoint Security for Linux
- **Aplicaciones de Kaspersky para máquinas virtuales:**
  - Kaspersky Security for Virtualization Light Agent
  - Kaspersky Security for Virtualization Agentless
- **Aplicaciones de Kaspersky para sistemas de correo y servidores SharePoint / de colaboración:**
  - Kaspersky Security for Linux Mail Server
  - Kaspersky Security for Microsoft Exchange Servers
- **Aplicaciones de Kaspersky para detección de ataques selectivos:**
  - Kaspersky Sandbox
  - Kaspersky Endpoint Detection and Response Optimum
  - Kaspersky Managed Detection and Response
- **Aplicaciones de Kaspersky para dispositivos con el sistema operativo KasperskyOS:**
  - Kaspersky IoT Secure Gateway
  - Kaspersky Security Management Suite (complemento para Kaspersky Thin Client)

*Para convertir directivas:*

1. En el árbol de consola, seleccione el Servidor de administración para el que desea convertir directivas.
2. En el menú contextual del Servidor de administración, seleccione **Todas las tareas → Asistente de conversión por lotes de directivas y tareas**.

Se inicia el Asistente de conversión por lotes de directivas y tareas. Siga las instrucciones del asistente.

Al concluir el asistente, se crearán nuevas directivas que utilicen los ajustes actuales definidos por el administrador y los ajustes nuevos de las versiones actualizadas de las aplicaciones de Kaspersky.

## Administración de perfiles de directivas

Un perfil de directiva es un conjunto determinado de configuraciones de una directiva activada en un dispositivo cliente (dispositivo móvil o equipo) cuando el dispositivo cumple reglas de activación especificadas. Al activarse un perfil se modifica la configuración de directiva que se encontraba activa en el dispositivo antes de que se activara el perfil. Dicha configuración tomará los valores que se habían especificado en el perfil.

Los perfiles de directiva permiten que los dispositivos de un mismo grupo de administración operen con diferentes configuraciones de directiva. Por ejemplo, puede presentarse una situación en la que sea necesario modificar la configuración de la directiva para algunos dispositivos de un grupo de administración. En ese caso, se pueden configurar perfiles de directiva para esa directiva, lo cual permitirá editar la configuración de la directiva para los dispositivos seleccionados del grupo de administración. Por ejemplo, la directiva prohíbe la ejecución de cualquier software de navegación por GPS en todos los dispositivos del grupo de administración de Usuarios. El software de navegación por GPS es necesario en un solo dispositivo del grupo de administración de Usuarios, en particular el que posee el usuario empleado como mensajero. Puede etiquetar ese dispositivo simplemente como "Mensajero" y configurar de nuevo el perfil de directiva de modo que permita que el software de navegación por GPS se ejecute solo en el dispositivo etiquetado como "Mensajero", conservando toda configuración de directivas restante. En ese caso, si un dispositivo etiquetado como "Mensajero" aparece en el grupo de administración de Usuarios, se podrá ejecutar el software de navegación por GPS. Sin la ejecución del software de navegación por GPS seguirá estando prohibida en otros dispositivos del grupo de administración de Usuarios a menos que estos también se etiqueten como "Mensajero".

Solo las siguientes directivas admiten perfiles:

- Directivas de Kaspersky Endpoint Security para Windows
- Directivas de Kaspersky Endpoint Security for Mac
- Directivas del complemento de Administración de dispositivos móviles de Kaspersky desde el Service Pack 1 de la versión 10 hasta el Service Pack 3 de la versión 10 Maintenance Release 1
- Directivas del complemento de Kaspersky Device Management for iOS
- Directivas de Kaspersky Security for Virtualization 5.1 Light Agent para Windows
- Directivas de Kaspersky Security for Virtualization 5.1 Light Agent para Linux

Los perfiles de directivas simplifican la administración de los dispositivos cliente a los que se aplican las directivas:

- La configuración de perfiles de directivas puede ser diferente de la configuración de las directivas.
- No es necesario que mantenga y aplique manualmente varias instancias de una sola directiva que difiera solamente en unos pocos parámetros.
- No tiene que asignar una directiva aparte para los usuarios que estén fuera de la oficina.
- Puede exportar e importar perfiles de directivas, así como crear perfiles de directivas nuevos según los existentes.
- Una sola directiva puede tener varios perfiles de directivas activos. Solo los perfiles que cumplen las reglas de activación en vigencia en el dispositivo se aplicarán a ese dispositivo.
- Los perfiles están sujetos a la jerarquía de la directiva. Una directiva heredada incluye todos los perfiles de la directiva de nivel superior.

## Prioridad de los perfiles

Los perfiles creados para una directiva se ordenan en forma descendente según su prioridad. Por ejemplo, si el perfil X está en una jerarquía mayor en la lista de perfiles que el perfil Y, el primero tiene mayor prioridad que el segundo. Es posible aplicar varios perfiles simultáneamente a un solo dispositivo. Cuando dos o más perfiles contienen valores diferentes para un mismo ajuste, el valor que se aplica en el dispositivo es el del perfil de mayor prioridad.

## Reglas de activación de perfiles

Un perfil de directiva se activa en un dispositivo cliente cuando se aplica una regla de activación. *Las reglas de activación* son un conjunto de condiciones que, cuando se cumplen, inician el perfil de directiva en un dispositivo. Una regla de activación puede contener las siguientes condiciones:

- Agente de red de un dispositivo cliente se conecta con el Servidor de administración con un conjunto dado de parámetros de conexión, como la dirección del Servidor, el número de puerto, etc.
- El dispositivo cliente no tiene conexión.
- Se ha asignado etiquetas específicas al dispositivo cliente.
- El dispositivo cliente pertenece a una unidad específica de Active Directory, sea esta pertenencia explícita (el dispositivo se encuentra directamente en la unidad especificada) o implícita (el dispositivo se encuentra en una unidad subordinada a la que se especificó, independientemente del nivel de anidamiento) ubicada en una unidad específica de Active Directory; el dispositivo o su propietario pertenecen a un grupo de seguridad de Active Directory.
- El dispositivo cliente le pertenece a un propietario especificado o el propietario del dispositivo está incluido en un grupo de seguridad interna de Kaspersky Security Center.
- Al propietario del dispositivo cliente se le ha asignado un rol específico.

## Directivas en la jerarquía de los grupos de administración

Si está creando una directiva en un grupo de administración de nivel bajo, esta directiva nueva hereda todos los perfiles de la directiva activa del grupo de nivel superior. Los perfiles con nombres idénticos se fusionan. Los perfiles de directivas del grupo de nivel superior tienen mayor prioridad. Por ejemplo, en el grupo de administración *A*, la directiva *P(A)* tiene los perfiles *X1*, *X2* y *X3* (en orden descendente de prioridad). En el grupo de administración *B*, que es un subgrupo del grupo *A*, la directiva *P(B)* se ha creado con los perfiles *X2*, *X4*, *X5*. Por lo tanto, la directiva *P(B)* se modificará junto con la directiva *P(A)*, de modo que la lista de perfiles de la directiva *P(B)* se verá así: *X1*, *X2*, *X3*, *X4*, *X5* (en orden descendente de prioridad). La prioridad del perfil *X2* dependerá del estado inicial de *X2* de la directiva *P(B)* y *X2* de la directiva *P(A)*. Después de crearse la directiva *P (B)*, la directiva *P (A)* ya no se muestra más en el subgrupo *B*.

La directiva activa se vuelve a calcular cada vez que inicia el Agente de red, se habilita y deshabilita el modo sin conexión o se edita la lista de etiquetas asignadas al dispositivo cliente. Por ejemplo, el tamaño de la RAM se ha aumentado en el dispositivo, lo cual, por su parte, ha activado el perfil de directiva que se aplica en los dispositivos con un tamaño grande de RAM.

## Propiedades y restricciones de los perfiles de directivas

Los perfiles tienen las siguientes propiedades:

- Los perfiles de una directiva inactiva no influyen en absoluto en los dispositivos cliente.
- Si se establece una directiva en el estado **Directiva para fuera de la oficina**, los perfiles de la directiva también se aplicarán cuando se desconecte un dispositivo de la red corporativa.
- Los perfiles no admiten el análisis estático del acceso a los archivos ejecutables.
- Un perfil de directiva no puede contener ninguna configuración de notificaciones de eventos.

- Si se utiliza el puerto UDP 15000 para la conexión de un dispositivo al Servidor de administración, el perfil de directiva correspondiente se activa en el plazo de un minuto desde que se asigna una etiqueta al dispositivo.
- Puede usar reglas para la conexión del Agente de red con el Servidor de administración al crear reglas de activación del perfil de directiva.

## Crear un perfil de directiva

Solo se pueden crear perfiles para las directivas de las siguientes aplicaciones:

- Kaspersky Endpoint Security 10 Service Pack 1 para Windows y versiones posteriores
- Kaspersky Endpoint Security 10 Service Pack 1 for Mac
- Complemento de Kaspersky Mobile Device Management versiones 10 Service Pack 1 hasta la 10 Service Pack 3 Maintenance Release 1
- Complemento de Kaspersky Device Management for iOS
- Kaspersky Security for Virtualization 5.1 Light Agent para Windows y Linux

*Para crear un perfil de directiva:*

1. En el árbol de consola, seleccione el grupo de administración para cuya directiva desea crear un perfil de directiva.
2. En el espacio de trabajo del grupo de administración, seleccione la pestaña **Directivas**.
3. Seleccione una directiva y, a través del menú contextual, abra la ventana de propiedades de la misma.
4. Abra la sección **Perfiles de directiva** en la ventana Propiedades de la directiva y haga clic en el botón **Agregar**.

   Se iniciará el Asistente de nuevos perfiles de directivas.
5. En la ventana **Nombre del perfil de directiva** del Asistente, especifique lo siguiente:

   a. Nombre del perfil de directiva

      El nombre de un perfil no puede contener más de 100 caracteres.

   b. Estado del perfil de directiva (*Habilitado* o *Deshabilitado*)

      La recomendamos que cree y habilite los perfiles de directivas inactivos solo después de que haya terminado completamente con la configuración y las condiciones de activación del perfil de directiva.
6. Marque la casilla **Deseo configurar la regla de activación para el perfil de directiva una vez que se cierre este Asistente** para iniciar el Asistente de nueva regla de activación para perfil de directiva. Siga los pasos del asistente.
7. Edite la configuración del perfil de directiva en la ventana de propiedades del perfil de directiva según sea necesario.
8. Guarde los cambios haciendo clic en **Aceptar**.

   El perfil se guarda. El perfil se activará en los dispositivos que cumplan con las reglas de activación.

Puede crear varios perfiles para una misma directiva. Los perfiles que se han creado para una directiva se muestran en las propiedades de la directiva, en la sección **Perfiles de directiva**. Puede modificar un perfil de directiva y cambiar la prioridad del perfil, así como también eliminar el perfil.

## Modificar un perfil de directiva

### Editar la configuración de un perfil de directiva

La posibilidad de modificar un perfil de directiva solo está disponible para las directivas de Kaspersky Endpoint Security para Windows.

*Para modificar un perfil de directiva:*

1. En el árbol de consola, seleccione el grupo de administración para el que se debe modificar el perfil de directiva.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Seleccione una directiva y, a través del menú contextual, abra la ventana de propiedades de la misma.
4. Abra la sección **Perfiles de directiva** en las propiedades de la directiva.

   Esta sección contiene una lista de perfiles que se han creado para la directiva. Los perfiles se muestran en la lista de acuerdo con sus prioridades.
5. Seleccione un perfil de directiva y haga clic en el botón **Propiedades**.
6. En la ventana de propiedades, configure el perfil:
   - Si es necesario, en la sección **General**, cambie el nombre del perfil, y habilite o deshabilite el perfil usando la casilla **Habilitar perfil**.
   - En la sección **Reglas de activación**, edite las reglas de activación del perfil.
   - Edite la configuración de la directiva en las secciones correspondientes.
7. Haga clic en **Aceptar**.

Los cambios de configuración entrarán en vigor cuando el dispositivo se sincronice con el Servidor de administración (si el perfil de directiva está activo) o cuando se accione una de las reglas de activación (si el perfil de directiva está inactivo).

### Cambiar la prioridad de un perfil de directiva

Las prioridades de los perfiles de directivas definen el orden de activación de los perfiles en un dispositivo cliente. Las prioridades se usan si se establecen reglas de activación idénticas para diferentes perfiles de directivas.

Por ejemplo, se han creado dos perfiles de directivas: *Perfil 1* y *Perfil 2*, que difieren en los valores respectivos de un solo parámetro (*Valor 1* y *Valor 2*). La prioridad del *Perfil 1* es más alta que la del *Perfil 2*. Además, también hay perfiles con prioridades más bajas que la del *Perfil 2*. Las reglas de activación de esos perfiles son idénticas.

Cuando se desencadena una regla de activación, se activará el *Perfil 1*. El parámetro en el dispositivo tomará el *Valor 1*. Si elimina el *Perfil 1*, el *Perfil 2* tendrá la prioridad más alta y el parámetro tomará el *Valor 2*.

En la lista de perfiles de directivas, los perfiles se muestran de acuerdo con sus prioridades respectivas. El perfil con la prioridad más alta ocupa el primer lugar. Para cambiar la prioridad de un perfil, use los botones de flecha arriba  y flecha abajo  .

## Eliminar un perfil de directiva

*Para eliminar un perfil de directiva:*

1. En el árbol de consola, seleccione el grupo de administración para el que desea eliminar un perfil de directiva.
2. En el espacio de trabajo del grupo de administración, seleccione la pestaña **Directivas**.
3. Seleccione una directiva y, a través del menú contextual, abra la ventana de propiedades de la misma.
4. Abra la sección **Perfiles de directiva** en las propiedades de la directiva de Kaspersky Endpoint Security.
5. Seleccione el perfil de directiva que desea eliminar y haga clic en el botón **Eliminar**.

Se elimina el perfil de directiva. El estado activo se transferirá a otro perfil de directiva cuyas reglas de activación se desencadenan en el dispositivo, o con la directiva.

## Crear una regla de activación para un perfil de directiva

*Para crear una regla de activación para un perfil de directiva:*

1. En el árbol de la consola, seleccione el grupo de administración para el que deba crear la regla de activación para perfil de directiva.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. Seleccione una directiva y, a través del menú contextual, abra la ventana de propiedades de la misma.
4. Vaya a la sección **Perfiles de directiva** en la ventana de propiedades de la directiva.
5. Seleccione el perfil de directiva para el cual deba crear la regla de activación. A continuación, haga clic en el botón **Propiedades**.

   Se abre la ventana de propiedades del perfil de directiva.

   Si la lista de perfiles de la directiva está vacía, puede crear un perfil de directiva.
6. Vaya a la sección **Reglas de activación** y haga clic en el botón **Agregar**.

   Se inicia el Asistente de nueva regla de activación para perfil de directiva.

7. En la ventana **Reglas de activación del perfil de directivas**, marque las casillas ubicadas junto a las condiciones que afectarán la activación del perfil de directiva que está creando:

- **Reglas generales para la activación del perfil de directiva**

  Marque esta casilla para configurar reglas que hagan que el perfil de directiva se active en un dispositivo dependiendo del estado del modo sin conexión de ese dispositivo, de las reglas de conexión con el Servidor de administración o de las etiquetas que el dispositivo tenga asignadas.

- **Reglas basadas en el uso de Active Directory**

  Marque esta casilla para configurar reglas que hagan que el perfil de directiva se active en un dispositivo si el mismo pertenece a una unidad organizativa de Active Directory en particular o si el dispositivo o su propietario son miembros de un grupo de seguridad de Active Directory.

- **Reglas basadas en el propietario del dispositivo**

  Marque esta casilla para configurar reglas que hagan que el perfil de directiva se active en un dispositivo dependiendo de quién sea su propietario.

- **Reglas para las especificaciones del hardware**

  Marque esta casilla para configurar reglas que hagan que el perfil de directiva se active en un dispositivo dependiendo de la cantidad de memoria y del número de procesadores lógicos que el dispositivo tenga.

El número de páginas adicionales del asistente dependerá de las opciones que haya elegido en el primer paso. Podrá modificar las reglas de activación del perfil de directiva más adelante.

8. En la ventana **Condiciones generales**, configure los siguientes parámetros:

- En el campo **El dispositivo no tiene conexión**, en la lista desplegable, elija una condición relativa a la presencia del dispositivo en la red:

  - **Sí**

    El dispositivo está en una red externa, lo que significa que el Servidor de administración no está disponible.

  - **No**

    El dispositivo está en la red, lo que significa que el Servidor de administración está disponible.

  - **Ningún valor seleccionado**

    El criterio no se aplicará.

- En el campo **El dispositivo está en la ubicación de red especificada**, use las listas desplegables para hacer que el perfil de directiva se active dependiendo de si la regla de conexión al Servidor de administración se ha ejecutado o no en el dispositivo:

  - **Ejecutada / No ejecutada**

    Condición para que se active el perfil de directiva (dependiendo de si la regla se ha ejecutado o no).

  - **Nombre de la regla**

    Descripción de ubicación de red para regular la conexión del dispositivo a un Servidor de administración, cuyas condiciones se deben cumplir (o no se deben cumplir) para la activación del perfil de directiva.

    Puede crear o configurar una descripción de ubicación de red de dispositivos para la conexión con un Servidor de administración en una regla de cambio de Agente de red.

La ventana **Condiciones generales** se mostrará si ha marcado la casilla **Reglas generales para la activación del perfil de directiva**.

9. En la ventana **Condiciones con etiquetas**, especifique la siguiente configuración:

- Lista de etiquetas

  En la lista de etiquetas, configure la regla que hará que los dispositivos que tengan ciertas etiquetas se incluyan en el perfil de directiva. Para configurar esta regla, active las casillas ubicadas junto a las etiquetas pertinentes.

  Si necesita agregar etiquetas nuevas, introdúzcalas en el campo que se encuentra sobre la lista y haga clic en el botón **Agregar**.

  El perfil de directiva incluirá aquellos dispositivos que, en su descripción, contengan todas las etiquetas seleccionadas. Si no activa estas casillas, no se aplicará este criterio. Estas casillas están desactivadas de manera predeterminada.

- Aplicar a los dispositivos que no tengan las etiquetas especificadas

  Habilite esta opción si tiene que invertir la selección de etiquetas.

  Si habilita esta opción, el perfil de directiva incluirá aquellos dispositivos que no tengan, en su descripción, ninguna de las etiquetas seleccionadas. Si deshabilita esta opción, no se aplicará el criterio.

  Esta opción está deshabilitada de forma predeterminada.

La ventana **Condiciones con etiquetas** se muestra si la casilla **Reglas generales para la activación del perfil de directiva** está seleccionada.

10. En la ventana **Condiciones que usan Active Directory**, especifique la siguiente configuración:

- Membrecía del propietario del dispositivo en un grupo de seguridad de Active Directory

  Si habilita esta opción, el perfil de directiva se activará en un dispositivo si su propietario es miembro del grupo de seguridad especificado. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

- Membrecía del dispositivo en un grupo de seguridad de Active Directory

  Si habilita esta opción, el perfil de directiva se activará en el dispositivo. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

- Asignación de dispositivos en la unidad organizativa de Active Directory

  Si habilita esta opción, el perfil de directiva se activará en un dispositivo si el mismo está incluido en la unidad organizativa de Active Directory especificada. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil.

  Esta opción está deshabilitada de forma predeterminada.

La ventana **Condiciones que usan Active Directory** se mostrará si marcó la casilla **Reglas basadas en el uso de Active Directory**.

11. En la ventana **Condiciones que usan el propietario del dispositivo**, especifique la siguiente configuración:

- **Propietario del dispositivo**

  Habilite esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo dependiendo de quién sea el propietario del mismo. En la lista desplegable bajo la casilla, seleccione el criterio que determinará la activación del perfil:

  - El dispositivo pertenece al propietario especificado (signo "=").
  - El dispositivo no pertenece al propietario especificado (signo "#").

    Si habilita esta opción, el perfil se activará en el dispositivo siguiendo el criterio configurado. Podrá señalar al propietario del dispositivo una vez que habilite la opción. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

- **El propietario del dispositivo está incluido en un grupo de seguridad interno**

  Habilite esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo dependiendo de si su propietario pertenece a un grupo de seguridad interno de Kaspersky Security Center. En la lista desplegable bajo la casilla, seleccione el criterio que determinará la activación del perfil:

  - El propietario del dispositivo es miembro del grupo de seguridad especificado (signo "=").
  - El propietario del dispositivo no es miembro del grupo de seguridad especificado (signo "#").

    Si habilita esta opción, el perfil se activará en el dispositivo siguiendo el criterio configurado. Podrá especificar el nombre de un grupo de seguridad de Kaspersky Security Center. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

- **Activar el perfil de directiva por rol específico del propietario del dispositivo**

  Habilite esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo dependiendo del rol asignado al propietario del mismo. Utilice la lista de roles existentes para agregar el rol en forma manual.

  Si habilita esta opción, el perfil se activará en el dispositivo siguiendo el criterio configurado.

La ventana **Condiciones que usan el propietario del dispositivo** muestra si la casilla **Reglas basadas en el propietario del dispositivo** específico está seleccionada.

12. En la ventana **Condiciones que usan las especificaciones del equipo**, especifique la siguiente configuración:

- **Tamaño de RAM, en MB**

  Habilite esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo en función de la cantidad de RAM que este posea. En la lista desplegable bajo la casilla, seleccione el criterio que determinará la activación del perfil:

  - El tamaño de la RAM del dispositivo está por debajo del valor especificado (signo "<").
  - El tamaño de la RAM del dispositivo está por encima del valor especificado (signo ">").

  Si habilita esta opción, el perfil se activará en el dispositivo siguiendo el criterio configurado. Podrá especificar la cantidad de RAM con la que deberá contar el dispositivo. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

- **Número de procesadores lógicos**

  Habilite esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo en función del número de procesadores lógicos que este tenga. En la lista desplegable bajo la casilla, seleccione el criterio que determinará la activación del perfil:

  - El número de procesadores lógicos del dispositivo es menor o igual que el valor especificado (signo "<").
  - El número de procesadores lógicos del dispositivo es mayor o igual que el valor especificado (signo ">").

  Si habilita esta opción, el perfil se activará en el dispositivo siguiendo el criterio configurado. Podrá especificar la cantidad de procesadores lógicos con los que deberá contar el dispositivo. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

Se muestra la ventana **Condiciones que usan las especificaciones del equipo** si se selecciona la casilla **Reglas para las especificaciones del hardware**.

13. En la ventana **Nombre de la regla de activación del perfil de directiva**, en el campo **Nombre de la regla**, escriba un nombre para la regla.

Se guardará el perfil. El perfil se activará en el dispositivo cuando se desencadenen las reglas de activación.

Las reglas de activación creadas para un perfil de directiva se muestran en las propiedades del perfil, dentro de la sección **Reglas de activación**. Puede modificar o eliminar cualquiera de las reglas de activación del perfil de directiva.

Existe la posibilidad de que varias reglas de activación se desencadenen simultáneamente.

# Reglas de movimiento de dispositivos

Recomendamos que automatice la asignación de dispositivos a grupos de administración usando las *reglas de movimiento de dispositivos*. Una regla de movimiento de dispositivos consta de tres partes principales: nombre, condición de ejecución (expresión lógica con atributos del dispositivo) y grupo de administración de destino. Una regla mueve un dispositivo al grupo de administración de destino si los atributos del dispositivo cumplen la condición de ejecución de la regla.

Toda regla de movimiento de dispositivos tiene una prioridad. El Servidor de administración comprueba si los atributos del dispositivo cumplen con la condición de ejecución de cada regla, en orden ascendente de prioridad. Si los atributos del dispositivo cumplen con la condición de ejecución de una regla, el dispositivo se mueve al grupo de destino, y con esto cesa el procesamiento de la regla en este dispositivo. Si los atributos de dispositivo cumplen con las condiciones de varias reglas, el dispositivo se mueve al grupo de destino de la regla con la prioridad más alta (es decir, la que tiene la clasificación más alta en la lista de reglas).

Las reglas de movimiento de dispositivos se pueden crear implícitamente. Por ejemplo, en las propiedades de un paquete de instalación o una tarea de instalación remota, puede especificar el grupo de administración al cual el dispositivo se debe mover después de que Agente de red se instala en este. Además, las reglas de movimiento de dispositivos pueden ser creadas explícitamente por el administrador de Kaspersky Security Center, en la lista de reglas de movimiento. La lista se localiza en la Consola de administración, en las propiedades del grupo de **Dispositivos no asignados**.

De forma predeterminada, la regla de movimiento está diseñada para la asignación inicial de dispositivos a grupos de administración, que se ejecuta una sola vez. La regla mueve dispositivos desde el grupo de **Dispositivos no asignados** solo una vez. Si un dispositivo se movió una vez mediante esta regla, la regla no lo volverá a mover, incluso si devuelve el dispositivo al grupo de **Dispositivos no asignados** manualmente. Este es el modo recomendado de aplicar las reglas de movimiento.

Puede mover dispositivos que ya se han asignado a algunos grupos de administración. Para hacer esto, en las propiedades de una regla, borre la casilla de verificación **Solo mover dispositivos que no pertenezcan a un grupo de administración**.

Aplicar reglas de movimiento a dispositivos que ya se han asignado a algunos grupos de administración aumenta considerablemente la carga en el Servidor de administración.

La casilla **Solo mover dispositivos que no pertenezcan a un grupo de administración** está bloqueada en las propiedades de las reglas de movimiento creadas automáticamente. Esas reglas se crean cuando agrega la tarea *Instalar la aplicación de forma remota* o crea un paquete de instalación independiente.

Puede crear una regla móvil que afectaría a un dispositivo solo repetidamente.

Recomendamos encarecidamente no mueva un solo dispositivo desde un grupo al otro repetidamente (por ejemplo, a fin de aplicar una directiva especial a ese dispositivo, ejecutar una tarea de grupo especial o actualizar el dispositivo a través de un punto de distribución específico).

Tales situaciones no se admiten, porque aumentan la carga en el Servidor de administración y el tráfico de red a un grado extremo. Estas situaciones también entran en conflicto con los principios operativos de Kaspersky Security Center (en particular en el área de derechos de acceso, eventos e informes). Se debe encontrar otra solución; por ejemplo, a través del uso de perfiles de directivas, tareas para selecciones de dispositivos, asignación de Agentes de red según el escenario estándar, entre otras cosas.

# Clonación de reglas de movimiento de dispositivos

Cuando tiene que crear varias reglas de movimiento de dispositivos con configuraciones similares, puede clonar una regla existente y luego cambiar la configuración de la regla clonada. Por ejemplo, esto es útil cuando debe tener varias reglas idénticas de movimiento de dispositivos con diferentes rangos de IP y grupos objetivo.

*Para clonar una regla móvil de dispositivo:*

1. Abra la ventana principal de la aplicación.
2. En la carpeta **Dispositivos no asignados**, haga clic en **Configurar reglas**.

   Se abrirá la ventana Propiedades: **Dispositivos no asignados**.
3. En la sección **Mover dispositivos**, seleccione la regla de movimiento del dispositivo que desea clonar.
4. Haga clic en **Regla de clonación**.

   Al final de la lista se añadirá un clon de la regla de movimiento del dispositivo seleccionado.

Se crea una nueva regla en el estado desactivado. Puede editar y activar la regla en cualquier momento.

# Categorización del software

La herramienta principal para supervisar la ejecución de aplicaciones son las *categorías de Kaspersky* (en adelante también conocidas como *categorías KL*). Las categorías de KL ayudan a los administradores de Kaspersky Security Center a simplificar la asistencia de la clasificación del software y minimizan el tráfico hacia los dispositivos administrados.

Las categorías de usuario solo se deben crear para aplicaciones que no se pueden clasificar en ninguna de las categorías KL existentes (por ejemplo, para el software personalizado). Las categorías de usuario se crean sobre la base de un paquete de instalación de la aplicación (MSI) o una carpeta con paquetes de instalación.

Si está disponible una colección grande de software que no se ha clasificado a través de categorías KL, puede ser útil crear una categoría actualizada automáticamente. Las sumas de control de archivos ejecutables automáticamente se agregarán a esta categoría en cada modificación de la carpeta que contiene paquetes de distribución.

No cree categorías de software actualizadas automáticamente para las carpetas Mis documentos, %windir%, %ProgramFiles% y %ProgramFiles(x86)%. El conjunto de archivos en estas carpetas está sujeto a cambios frecuentes, lo que lleva a una carga aumentada en el Servidor de administración y tráfico de red aumentado. Debe crear una carpeta dedicada con la colección de software y periódicamente agregar elementos nuevos elementos a ella.

# Requisitos previos para instalar aplicaciones en dispositivos de una organización cliente

El proceso de la instalación remota de las aplicaciones en dispositivos de una organización cliente es idéntico al proceso de instalación remota en una empresa.

Para instalar las aplicaciones en los dispositivos de una organización cliente, deben seguirse los siguientes pasos:

- Antes de instalar por primera vez las aplicaciones en los dispositivos de la organización cliente, instale el Agente de red en ellas.

  Cuando la configuración del paquete de instalación del Agente de red en Kaspersky Security Center es realizado por el proveedor de servicio, ajuste los siguientes parámetros en la ventana de propiedades del paquete de instalación:

  - En la sección **Conexión**, en la cadena **Servidor de administración**, especifique la dirección del mismo Servidor de administración virtual que se especificó durante la instalación local del Agente de red en el punto de distribución.

  - En la sección **Avanzado**, seleccione la casilla de verificación **Conectarse al Servidor de administración mediante una puerta de enlace de conexión**. En la cadena **Dirección de la puerta de enlace**, especifique la dirección del punto de distribución. Puede usar la dirección IP o el nombre del dispositivo en la red de Windows.

- Seleccione **Utilización de recursos del sistema operativo mediante puntos de distribución** como método de descarga para el paquete de instalación del Agente de red. Puede seleccionar el método de descarga de la siguiente manera:

  - Si instala la aplicación usando la tarea de instalación remota, puede especificar el método de descarga de una de las siguientes maneras:

    - Al crear una tarea de instalación remota en la ventana **Configuración**.

    - En la ventana de propiedades de la tarea de instalación remota, en la sección **Configuración**.

  - Si instala aplicaciones con el Asistente de instalación remota, puede seleccionar el método de descarga en la ventana **Configuración** de este Asistente.

- La cuenta usada por el punto de distribución para la autorización debe tener acceso al recurso Admin$ en todos los dispositivos cliente.

# Ver y modificar la configuración local de la aplicación

El sistema de administración de Kaspersky Security Center permite la administración remota de la configuración local de la aplicación en dispositivos a través de la Consola de administración.

*La configuración local de la aplicación* se refiere a la configuración de una aplicación, específica para un dispositivo. Puede usar Kaspersky Security Center para especificar la configuración local de una aplicación en dispositivos incluidos en los grupos de administración.

Las descripciones detalladas de la configuración de aplicaciones Kaspersky se proporcionan en las guías respectivas.

*Para ver o modificar la configuración local de la aplicación:*

1. En el espacio de trabajo del grupo al que pertenece el dispositivo requerido, seleccione la pestaña **Dispositivos**.
2. En la ventana de propiedades del dispositivo, en la sección **Aplicaciones**, seleccione la aplicación relevante.
3. Abra la ventana de propiedades de la aplicación mediante doble clic en el nombre de la aplicación o con un clic en el botón **Propiedades**.

   Se abrirá la ventana de configuración local de la aplicación seleccionada, de modo que pueda ver y editar esa configuración.

Puede cambiar los valores de la configuración que no tienen prohibida la modificación mediante una directiva de grupo (es decir, aquellos valores no marcados con el ícono de candado (🔒) en una directiva).

# Actualización de Kaspersky Security Center y de las aplicaciones administradas

Esta sección describe los pasos que debe seguir para actualizar Kaspersky Security Center y las aplicaciones administradas.

## Procedimiento: actualización regular de bases de datos y aplicaciones de Kaspersky

En esta sección, se detalla un escenario para actualizar regularmente las bases de datos, los módulos de software y las aplicaciones de Kaspersky. Una vez que complete el escenario para configurar la protección de la red, deberá mantener la fiabilidad del sistema de protección. Esto garantizará que los servidores de administración y los dispositivos administrados siempre estén protegidos contra virus, ataques de red, ataques de phishing y otras amenazas.

Para que la protección de la red mantenga su eficacia, debe actualizar periódicamente lo siguiente:

- Las bases de datos y los módulos de software de Kaspersky
- Las aplicaciones de Kaspersky que se encuentren instaladas, incluidas las aplicaciones de seguridad y los componentes de Kaspersky Security Center

Al concluir este escenario, tendrá las siguientes certezas:

- Su red está protegida por el software más reciente de Kaspersky, incluidos los componentes de Kaspersky Security Center y las aplicaciones de seguridad.
- Las bases de datos antivirus y otras bases de datos de Kaspersky críticas para la seguridad de la red estarán siempre actualizadas.

## Requisitos previos

Los dispositivos administrados deben tener conexión con el Servidor de administración. Si no tienen conexión, considere actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky de forma manual o directa desde los servidores de actualización de Kaspersky.

El Servidor de administración debe tener conexión a Internet.

Antes de comenzar, compruebe que hizo lo siguiente:

1. Desplegó las aplicaciones de seguridad de Kaspersky en los dispositivos administrados siguiendo las instrucciones del escenario para desplegar aplicaciones de Kaspersky a través de Kaspersky Security Center Web Console.

2. Creó y configuró todas las directivas, perfiles de directivas y tareas que se requieren según el escenario para configurar la protección de red.

3. Asignó una cantidad apropiada de puntos de distribución de acuerdo con la cantidad de dispositivos administrados y la topología de la red.

El proceso para actualizar las bases de datos y las aplicaciones de Kaspersky se divide en etapas:

1. **Elegir un esquema de actualización**

   Existen distintos esquemas para instalar las actualizaciones para los componentes de Kaspersky Security Center y las aplicaciones de seguridad. Elija el esquema o varios esquemas que cumplan con los requisitos de su red.

2. **Crear la tarea para descargar actualizaciones en el repositorio del Servidor de administración**

   Esta tarea se crea automáticamente con el asistente de inicio rápido de Kaspersky Security Center. Si no ejecutó el asistente, cree la tarea ahora.

   Esta tarea se necesita para descargar actualizaciones de los servidores de actualizaciones de Kaspersky y guardarlas en el repositorio del Servidor de administración. También se la requiere para actualizar las bases de datos y los módulos de software de Kaspersky correspondientes a Kaspersky Security Center. Una vez descargadas, las actualizaciones se pueden propagar a los dispositivos administrados.

   Si su red tiene puntos de distribución asignados, las actualizaciones se descargan automáticamente desde el repositorio del Servidor de administración a los repositorios de los puntos de distribución. En este caso, los dispositivos administrados incluidos en el alcance de un punto de distribución descargan las actualizaciones desde el repositorio del punto de distribución en lugar del repositorio del Servidor de administración.

   Instrucciones:

   - Consola de administración: Creación de la tarea para descargar actualizaciones en el repositorio del Servidor de administración
   - Kaspersky Security Center Web Console: Creación de la tarea para descargar actualizaciones en el repositorio del Servidor de administración

3. **Crear la tarea para descargar actualizaciones en los repositorios de los puntos de distribución (opcional)**

   De forma predeterminada, las actualizaciones se descargan a los puntos de distribución desde el Servidor de administración. Puede configurar Kaspersky Security Center para descargar las actualizaciones a los puntos de distribución directamente desde los servidores de actualización de Kaspersky. Descargar las actualizaciones en los repositorios de los puntos de distribución es preferible cuando el Servidor de administración no tiene acceso a Internet o cuando transmitir datos entre el Servidor de administración y los puntos de distribución es más costoso que transmitir datos entre los puntos de distribución y los servidores de actualizaciones de Kaspersky.

Si hay puntos de distribución asignados en su red y se creó la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*, los puntos de distribución descargarán las actualizaciones de los servidores de actualizaciones de Kaspersky y no del repositorio del Servidor de administración.

Instrucciones:

- Consola de administración: Creación de la tarea para descargar actualizaciones en los repositorios de los puntos de distribución
- Kaspersky Security Center Web Console: Creación de la tarea para descargar actualizaciones en los repositorios de los puntos de distribución

4. **Configurar los puntos de distribución**

   Si su red tiene puntos de distribución asignados, asegúrese de que la opción **Desplegar actualizaciones** esté habilitada en las propiedades de todos los puntos de distribución pertinentes. Si deja esta opción está deshabilitada en un punto de distribución, los dispositivos incluidos en el alcance del mismo obtendrán sus actualizaciones del repositorio del Servidor de administración.

   Si desea que los dispositivos administrados reciban sus actualizaciones solamente de los puntos de distribución, habilite la opción **Distribuir archivos solo a través de los puntos de distribución** en la directiva del Agente de red.

5. **Habilitar la descarga de actualizaciones sin conexión o el uso de archivos diff para optimizar el proceso de actualización (opcional)**

   Puede optimizar el proceso de actualización utilizando el modelo de descarga de actualizaciones sin conexión (habilitado de forma predeterminada) o utilizando archivos diff. Para cada segmento de red, debe elegir cuál de estas dos características habilitar, ya que no pueden funcionar simultáneamente.

   Cuando el modelo de descarga de actualizaciones sin conexión está habilitado, el Agente de red descarga las actualizaciones necesarias en el dispositivo administrado una vez que las actualizaciones se descargan en el repositorio del Servidor de administración, antes de que la aplicación de seguridad solicite las actualizaciones. Esto mejora la fiabilidad del proceso de actualización. Para usar este modelo, habilite la opción **Descargar actualizaciones y bases de datos antivirus del Servidor de administración con anticipación (recomendado)** en la directiva del Agente de red.

   Si no utiliza el modelo de descarga de actualizaciones sin conexión, puede optimizar el tráfico entre el Servidor de administración y los dispositivos administrados mediante el uso de archivos diff. Cuando esta función está habilitada, el Servidor de administración o un punto de distribución descarga archivos diferenciales en lugar de archivos completos de bases de datos o módulos de software de Kaspersky. Un archivo diff describe las diferencias entre dos versiones de un archivo de una base de datos o de un módulo de software. Por lo tanto, un archivo diff ocupa menos espacio que un archivo completo. Esto reduce el tráfico entre el Servidor de administración o los puntos de distribución y los dispositivos administrados. Para usar esta función, habilite la opción **Descargar archivos diff** en las propiedades de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* o *Descargar actualizaciones en los repositorios de los puntos de distribución*.

   Instrucciones:

   - Usar archivos diff para actualizar las bases de datos y los módulos de software de Kaspersky
   - Consola de administración: Habilitación y deshabilitación del modelo de descarga de actualizaciones sin conexión
   - Kaspersky Security Center Web Console: Habilitación y deshabilitación del modelo de descarga de actualizaciones sin conexión

6. **Verificación de las actualizaciones descargadas (opcional)**

Antes de instalar las actualizaciones descargadas, puede controlarlas con la tarea *Verificación de actualizaciones*. Esta tarea ejecuta de forma secuencial las tareas de actualización de dispositivos y las tareas de análisis antimalware configuradas a través de ajustes definidos para un grupo específico de dispositivos de prueba. Basándose en los resultados de la tarea, el Servidor de administración inicia o bloquea la propagación de las actualizaciones a los dispositivos restantes.

La tarea *Verificación de actualizaciones* puede ejecutarse como parte de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. En las propiedades de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, habilite la opción **Verificar actualizaciones antes de distribuirlas** en la Consola de administración o la opción **Ejecutar verificación de actualizaciones** en Kaspersky Security Center Web Console.

Instrucciones:

- Consola de administración: Verificación de las actualizaciones descargadas
- Kaspersky Security Center Web Console: Verificación de las actualizaciones descargadas

7. **Aprobar y rechazar actualizaciones de software**

   De forma predeterminada, las actualizaciones de software descargadas tienen el estado *Sin definir*. Puede cambiar este estado a *Aprobada* o *Rechazada*. Las actualizaciones aprobadas siempre se instalan. Si una actualización exige revisar y aceptar los términos del Contrato de licencia de usuario final, es necesario aceptar esos términos para proceder con la instalación. Una vez que se aceptan los términos, la actualización se puede propagar a los dispositivos administrados. Las actualizaciones de estado indefinido solo se pueden instalar en el Agente de red y en otros componentes de Kaspersky Security Center si así lo permite la configuración de la directiva del Agente de red. Las actualizaciones a las que se les asigna el estado *Rechazada* no se instalan en los dispositivos. Si previamente se instaló una actualización rechazada para una aplicación de seguridad, Kaspersky Security Center intentará desinstalar la actualización de todos los dispositivos.

   Aprobar y rechazar actualizaciones solo está disponible para el Agente de red y las aplicaciones de Kaspersky administradas instaladas en dispositivos cliente basados en Windows y en Linux. No se admite la actualización sin interrupciones del Servidor de administración, Kaspersky Security Center Web Console y los complementos web de administración.

   Instrucciones:

   - Consola de administración: Aprobar y rechazar actualizaciones de software
   - Kaspersky Security Center Web Console: Aprobar y rechazar actualizaciones de software

8. **Configurar la instalación automática de actualizaciones y parches para los componentes de Kaspersky Security Center**

   Las actualizaciones y los parches que se descargan para el Agente de red y para los demás componentes de Kaspersky Security Center se instalan automáticamente. Si deja habilitada la opción **Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes** en las propiedades del Agente de red, se instalarán todas las actualizaciones que se descarguen en el repositorio (o en los repositorios). Si deshabilita esta opción, los parches de Kaspersky que se descarguen y que tengan el estado *Sin definir* se instalarán únicamente si cambia su estado a *Aprobada*.

   Instrucciones:

   - Consola de administración: Habilitar y deshabilitar la actualización automática y la aplicación de parches para los componentes de Kaspersky Security Center
   - Kaspersky Security Center Web Console: Habilitar y deshabilitar la actualización automática y la aplicación de parches para los componentes de Kaspersky Security Center

9. **Instalación de actualizaciones para el Servidor de administración**

Las actualizaciones de software para el Servidor de administración no dependen de los estados de actualización. No se instalan automáticamente y deben ser aprobadas previamente por el administrador en la pestaña **Supervisión** en la Consola de administración (**Servidor de administración** `<nombre del servidor>` → **Supervisión**) o en la sección **Notificaciones** en Kaspersky Security Center Web Console (**Supervisión e informes** → **Notificaciones**). Después de eso, el administrador debe ejecutar explícitamente la instalación de las actualizaciones.

10. **Configurar la instalación automática de actualizaciones para las aplicaciones de seguridad**

    Cree tareas *Actualizar* para las aplicaciones administradas a fin de mantener al día las aplicaciones, los módulos de software y las bases de datos de Kaspersky (incluidas las bases de datos antivirus). Para evitar demoras en la instalación de actualizaciones, recomendamos que seleccione la opción **Al descargar nuevas actualizaciones al repositorio** al configurar la programación de la tarea.

    Si su red incluye dispositivos solo IPv6 y quiere actualizar regularmente las aplicaciones de seguridad instaladas en dichos dispositivos, asegúrese de que el Servidor de administración (versión 13.2 en adelante) y el Agente de red (versión 13.2 en adelante) estén instalados en los dispositivos administrados.

    De forma predeterminada, las actualizaciones para Kaspersky Endpoint Security para Windows y Kaspersky Endpoint Security para Linux se instalan solo si su estado se cambia a *Aprobada*. Puede cambiar los ajustes de actualización en la tarea *Actualizar*.

    Si una actualización exige revisar y aceptar los términos del Contrato de licencia de usuario final, es necesario aceptar esos términos para proceder con la instalación. Una vez que se aceptan los términos, la actualización se puede propagar a los dispositivos administrados.

    Instrucciones:

    - Consola de administración: Instalación automática de actualizaciones de Kaspersky Endpoint Security en los dispositivos
    - Kaspersky Security Center Web Console: Instalación automática de actualizaciones de Kaspersky Endpoint Security en los dispositivos

### Resultados

Al culminar este escenario, Kaspersky Security Center estará configurado para actualizar las bases de datos de Kaspersky y las aplicaciones de Kaspersky instaladas una vez que las actualizaciones se descarguen en el repositorio del Servidor de administración o en los repositorios de los puntos de distribución. Su siguiente tarea consistirá, entonces, en supervisar el estado de la red.

# Acerca de la actualización de las bases de datos, los módulos de software y las aplicaciones de Kaspersky

Para asegurarse de que la protección de sus servidores de administración y sus dispositivos administrados siempre esté al día, debe proporcionar actualizaciones para los siguientes elementos oportunamente:

- Las bases de datos y los módulos de software de Kaspersky

Antes de descargar las bases de datos y los módulos de software de Kaspersky, Kaspersky Security Center verifica que haya acceso a los servidores de Kaspersky. Si los servidores DNS configurados en el sistema no permiten acceder a los servidores de Kaspersky, la aplicación utiliza servidores DNS públicos. Esto se hace para garantizar que las bases de datos antivirus se mantengan actualizadas y para que los dispositivos administrados no vean afectado su nivel de seguridad.

- Las aplicaciones de Kaspersky que se encuentren instaladas, incluidas las aplicaciones de seguridad y los componentes de Kaspersky Security Center

  Kaspersky Security Center le permite actualizar el Agente de red y las aplicaciones de Kaspersky instaladas en dispositivos cliente basados en Windows y en Linux automáticamente. No se admite la actualización sin interrupciones del Servidor de administración, Kaspersky Security Center Web Console y los complementos web de administración. Para actualizar estos componentes, debe descargar las últimas versiones desde el sitio web de Kaspersky y realizar la instalación manualmente.

Existen distintos esquemas para descargar las actualizaciones necesarias y distribuirlas a los dispositivos administrados. La elección de una u otra opción depende de la configuración de la red. Estas son las posibilidades:

- Utilizar una sola tarea: *Descargar actualizaciones en el repositorio del Servidor de administración*
- Utilizar dos tareas:
  - la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*
  - La tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*
- Utilizar una carpeta local, una carpeta compartida o un servidor FTP (método manual)
- Realizar una descarga directa desde los servidores de actualizaciones de Kaspersky a Kaspersky Endpoint Security en los dispositivos administrados
- Utilizar una carpeta local o de red si el Servidor de administración no tiene conexión a Internet

## Utilizando la tarea Descargar actualizaciones en el repositorio del Servidor de administración

En este esquema, Kaspersky Security Center descarga las actualizaciones a través de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. En redes pequeñas que contienen menos de trescientos dispositivos administrados en un solo segmento de red o menos de diez dispositivos administrados en cada segmento de red, las actualizaciones se distribuyen a los dispositivos administrados directamente desde el repositorio del Servidor de administración (vea la siguiente imagen).



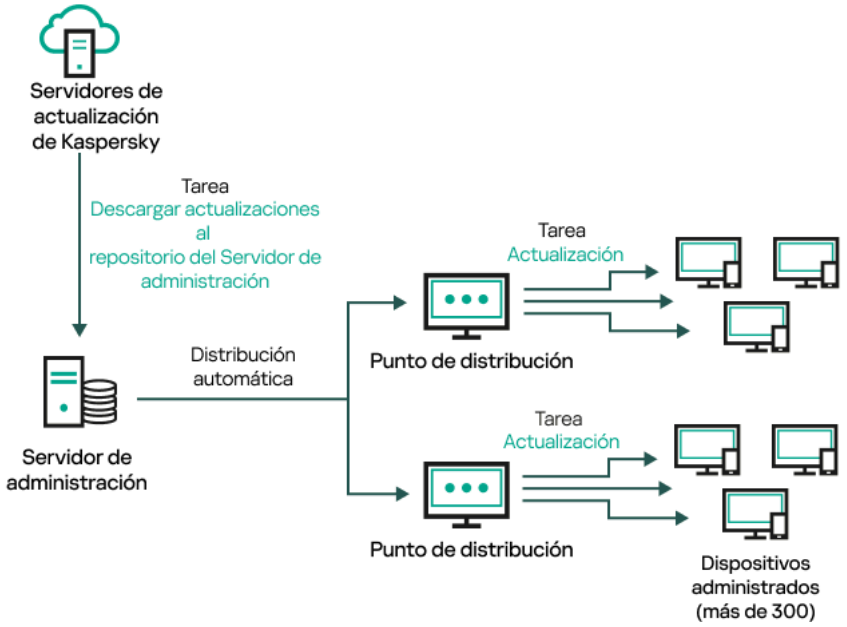

Actualización con la tarea Descargar actualizaciones en el repositorio del Servidor de administración sin utilizar puntos de distribución

De forma predeterminada, el Servidor de administración utiliza el protocolo HTTPS para comunicarse con los servidores de actualizaciones de Kaspersky y descargar las actualizaciones. Si lo desea, puede hacer que el

Servidor de administración utilice el protocolo HTTP en lugar del protocolo HTTPS.

Si su red contiene más de trescientos dispositivos administrados en un solo segmento de red (o si su red consta de varios segmentos de red con más de nueve dispositivos administrados por segmento), le recomendamos que utilice puntos de distribución para propagar las actualizaciones a los dispositivos administrados (vea la siguiente imagen). Los puntos de distribución reducen la carga del Servidor de administración y optimizan el flujo de tráfico entre el Servidor de administración y los dispositivos administrados. Puede determinar cuántos puntos de distribución necesitará para su red y cuál deberá ser su configuración.

En este esquema, las actualizaciones se descargan automáticamente del repositorio del Servidor de administración a los repositorios de los puntos de distribución. Los dispositivos administrados incluidos en el alcance de un punto de distribución descargan las actualizaciones del repositorio de ese punto de distribución en lugar del repositorio del Servidor de administración.




Actualización con puntos de distribución y la tarea Descargar actualizaciones en el repositorio del Servidor de administración

Al completarse la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, se descargan las siguientes actualizaciones al repositorio del Servidor de administración:

- Bases de datos y módulos de software de Kaspersky para Kaspersky Security Center

  Estas actualizaciones se instalan automáticamente.

- Bases de datos y módulos de software de Kaspersky para las aplicaciones de seguridad instaladas en los dispositivos administrados

  Estas actualizaciones se instalan a través de la tarea "Actualizar" de Kaspersky Endpoint Security para Windows.

- Actualizaciones para el Servidor de administración

  Estas actualizaciones no se instalan automáticamente. El administrador debe aprobarlas e instalarlas manualmente.

  Se requieren derechos de administrador local para instalar parches en el Servidor de administración.

- Actualizaciones para los componentes de Kaspersky Security Center

  Por defecto, estas actualizaciones se instalan automáticamente. Puede cambiar este comportamiento en la directiva del Agente de red.

- Actualizaciones para las aplicaciones de seguridad

  De forma predeterminada, Kaspersky Endpoint Security for Windows instala solo las actualizaciones que usted aprueba. Puede aprobar las actualizaciones mediante la Consola de administración o mediante Kaspersky Security Center Web Console. Las actualizaciones se instalan a través de la tarea *Actualizar* y se pueden configurar en las propiedades de dicha tarea.

La tarea *Descargar actualizaciones en el repositorio del Servidor de administración* no está disponible en servidores de administración virtuales. El repositorio del Servidor de administración virtual muestra las actualizaciones descargadas al Servidor de administración principal.

Si lo desea, puede verificar el buen funcionamiento de las actualizaciones en un conjunto de dispositivos de prueba. De no encontrarse errores durante la verificación, las actualizaciones se distribuirán a otros dispositivos administrados.

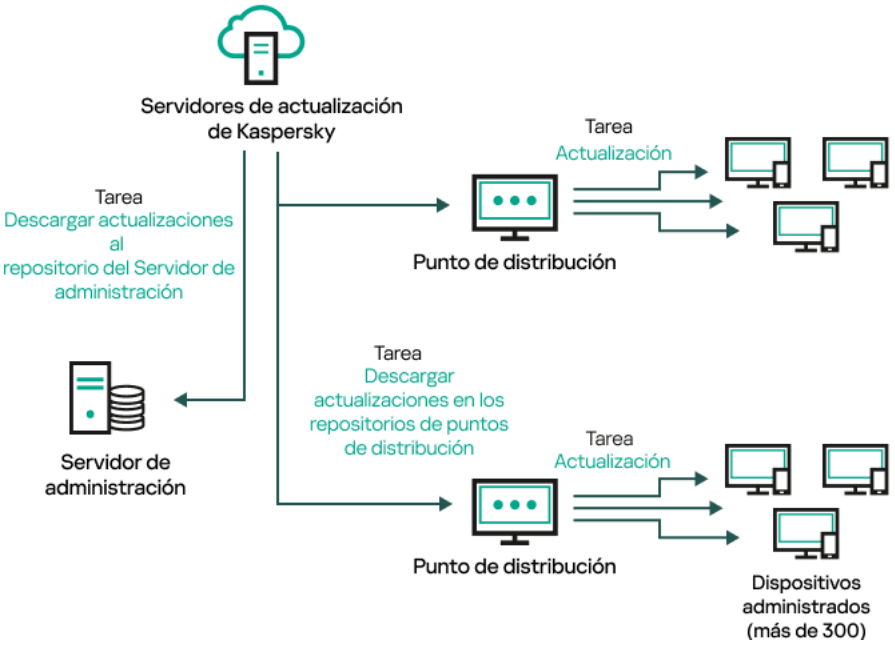
Cada aplicación de Kaspersky le solicita al Servidor de administración las actualizaciones que requiere. El Servidor de administración combina las solicitudes y descarga solo aquellas actualizaciones que han sido solicitadas por alguna aplicación. De este modo, se evita descargar la misma actualización más de una vez o descargar actualizaciones innecesarias. Para descargar las versiones correctas de las bases de datos y los módulos de software de Kaspersky, cuando se ejecuta la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, el Servidor de administración envía la siguiente información a los servidores de actualizaciones de Kaspersky automáticamente:

- Id. y versión de la aplicación
- Id. de instalación de la aplicación
- Id. de la clave activa
- Id. de ejecución de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*

La información transmitida no contiene datos personales ni confidenciales de ningún tipo. AO Kaspersky Lab protege la información conforme a las exigencias de la ley.

## Utilizar dos tareas: la tarea Descargar actualizaciones en el repositorio del Servidor de administración y la tarea Descargar actualizaciones en los repositorios de los puntos de distribución

Las actualizaciones pueden descargarse a los repositorios de los puntos de distribución directamente desde los servidores de actualizaciones de Kaspersky (y no desde el repositorio del Servidor de administración) y, una vez descargadas, pueden distribuirse a los dispositivos administrados (vea la siguiente imagen). Descargar las actualizaciones en los repositorios de los puntos de distribución es preferible cuando el Servidor de administración no tiene acceso a Internet o cuando transmitir datos entre el Servidor de administración y los puntos de distribución es más costoso que transmitir datos entre los puntos de distribución y los servidores de actualizaciones de Kaspersky.




Actualización con la tarea Descargar actualizaciones en el repositorio del Servidor de administración y la tarea Descargar actualizaciones en los repositorios de los puntos de distribución

De forma predeterminada, el Servidor de administración y los puntos de distribución se comunican con los servidores de actualizaciones de Kaspersky y descargan las actualizaciones utilizando el protocolo HTTPS. Puede hacer que el Servidor de administración y/o los puntos de distribución utilicen el protocolo HTTP en lugar del protocolo HTTPS.

Para implementar este esquema, cree la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución* además de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. Tras ello, los puntos de distribución descargarán las actualizaciones de los servidores de actualizaciones de Kaspersky y no del repositorio del Servidor de administración.

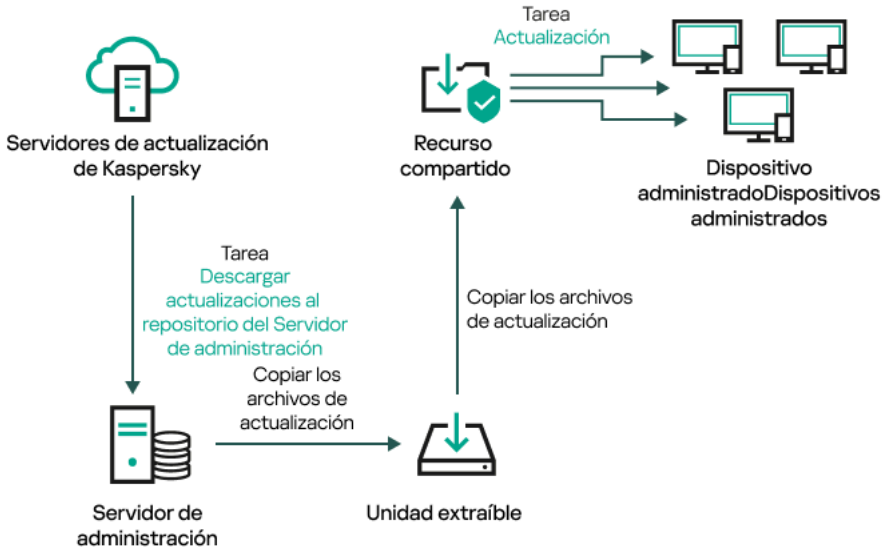
Los puntos de distribución con macOS no pueden descargar actualizaciones de los servidores de actualizaciones de Kaspersky.

Si hay uno o más dispositivos con macOS en el alcance de la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*, la tarea terminará con el estado *Error* aunque se complete sin errores en todos los dispositivos con Windows.

La tarea *Descargar actualizaciones en el repositorio del Servidor de administración* también es necesaria para este esquema, ya que se la utiliza para descargar las bases de datos y los módulos de software de Kaspersky para Kaspersky Security Center.

## Utilizar una carpeta local, una carpeta compartida o un servidor FTP (método manual)

Si sus dispositivos cliente no tienen conexión con el Servidor de administración, puede usar una carpeta local o un recurso compartido como origen de actualizaciones para actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky. De elegir esta alternativa, deberá copiar las actualizaciones requeridas del repositorio del Servidor de administración a una unidad extraíble y, luego, tendrá que copiar esas actualizaciones a la carpeta local o al recurso compartido que haya configurado como origen de actualizaciones en Kaspersky Endpoint Security (vea la siguiente imagen).



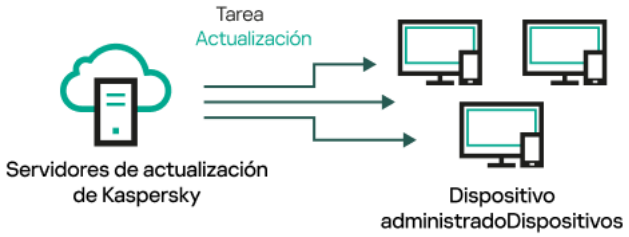

Actualización con una carpeta local, una carpeta compartida o un servidor FTP

Para obtener más información sobre los orígenes de actualizaciones en Kaspersky Endpoint Security, consulte los siguientes documentos de ayuda:

- Ayuda de Kaspersky Endpoint Security para Windows
- Ayuda de Kaspersky Endpoint Security for Linux

## Realizar una descarga directa desde los servidores de actualizaciones de Kaspersky a Kaspersky Endpoint Security en los dispositivos administrados

Puede configurar Kaspersky Endpoint Security en los dispositivos administrados para que la aplicación obtenga sus actualizaciones directamente de los servidores de actualizaciones de Kaspersky (vea la siguiente imagen).




Actualización directa de las aplicaciones de seguridad utilizando los servidores de actualizaciones de Kaspersky

En este esquema, la aplicación de seguridad no utiliza los repositorios que brinda Kaspersky Security Center. Para que las actualizaciones se descarguen directamente de los servidores de actualizaciones de Kaspersky, deberá definir esos servidores como origen de actualizaciones en la interfaz de la aplicación de seguridad. Para obtener más información acerca de estos ajustes, consulte los siguientes documentos de ayuda:

- Ayuda de Kaspersky Endpoint Security para Windows
- Ayuda de Kaspersky Endpoint Security for Linux

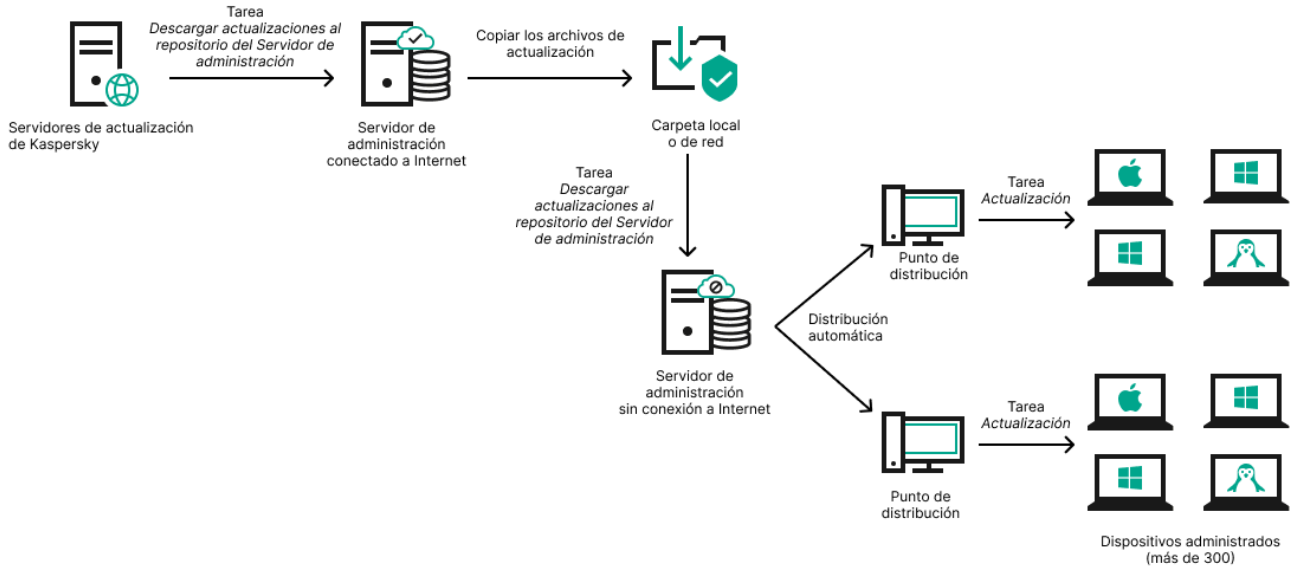
### Utilizar una carpeta local o de red si el Servidor de administración no tiene conexión a Internet

Si el Servidor de administración no tiene conexión a Internet, puede configurar la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* para descargar actualizaciones desde una carpeta local o de red. En este caso, de vez en cuando debe copiar los archivos de actualización necesarios en la carpeta especificada. Por ejemplo, puede copiar los archivos de actualización necesarios desde uno de los siguientes orígenes:

- Servidor de administración que cuente con una conexión a Internet (ver la figura a continuación)

  Dado que un Servidor de administración descarga solo las actualizaciones que solicitan las aplicaciones de seguridad, los conjuntos de aplicaciones de seguridad administrados por los Servidores de administración (el que tiene conexión a Internet y el que no) deben coincidir.

  Si el Servidor de administración que usa para descargar actualizaciones tiene la versión 13.2 o anterior, abra las propiedades de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* y, a continuación, habilite la opción **Descargar las actualizaciones usando el esquema antiguo**.




Utilizar una carpeta local o de red si el Servidor de administración no tiene conexión a Internet

- Kaspersky Update Utility

  Debido a que esta utilidad utiliza el antiguo esquema para descargar actualizaciones, abra las propiedades de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* y, a continuación, habilite la opción **Descargar las actualizaciones usando el esquema antiguo**.

## Acerca de la utilización de archivos diff para actualizar las bases de datos y los módulos de software de Kaspersky

Cuando Kaspersky Security Center descarga actualizaciones de los servidores de actualización de Kaspersky, optimiza el tráfico mediante el uso de archivos diff. También puede habilitar el uso de archivos diff por dispositivos (Servidores de administración, puntos de distribución y dispositivos cliente) que aceptan actualizaciones de otros dispositivos en su red.

## Acerca de la característica de descarga de archivos diff

Un archivo diff describe las diferencias entre dos versiones de un archivo de una base de datos o de un módulo de software. El uso de archivos diff ahorra tráfico dentro de la red de su empresa porque los archivos diff ocupan menos espacio que los archivos completos de bases de datos y módulos de software. Si la función de *descarga de archivos diff* está habilitada en el Servidor de administración o un punto de distribución, los archivos diff se guardan en este Servidor de administración o punto de distribución. Como resultado, los dispositivos que toman actualizaciones de este Servidor de administración o punto de distribución pueden usar los archivos diff guardados para actualizar sus bases de datos y módulos de software.

Para optimizar el uso de los archivos diff, le recomendamos que sincronice el programa de actualización de los dispositivos con el programa de actualización del Servidor de administración o el punto de distribución desde el cual los dispositivos reciben actualizaciones. Sin embargo, el tráfico se puede guardar incluso si los dispositivos se actualizan varias veces con menos frecuencia que el Servidor de administración o el punto de distribución desde el que reciben actualizaciones los dispositivos.

La función de descarga de archivos diff solo se puede activar en los Servidores de administración y los puntos de distribución de las versiones a partir de la versión 11. Si tiene servidores de administración y puntos de distribución de versiones anteriores y desea guardar archivos diff en ellos, actualícelos a la versión 11 o una posterior.

La función de descarga de archivos diff es incompatible con el modelo sin conexión de la descarga de actualizaciones. Significa que los Agentes de red que usan el modelo sin conexión de la descarga de actualizaciones no descargan archivos diff, incluso si la función de descarga de archivos diff está activada en el Servidor de administración o el punto de distribución que entrega actualizaciones a estos Agentes de redes.

Los puntos de distribución no utilizan la multidifusión IP para la distribución automática de archivos diff.

# Habilitación de la función de descarga de archivos diff

## Requisitos previos

Los requisitos previos para el escenario son los siguientes:

- Los servidores de administración y los puntos de distribución deben haberse actualizado a la versión 11 o una versión posterior.
- El modelo sin conexión de la descarga de actualizaciones está desactivado en la configuración de la directiva del Agente de red.

## Etapas

1. **Habilitar la función en el Servidor de administración**

   Habilite la función en la configuración de las actualizaciones de descarga en el repositorio de la tarea del Servidor de administración.

2. **Habilite la función para un punto de distribución**

Habilite la función para un punto de distribución que recibe actualizaciones a través de la tarea Descargar actualizaciones en los repositorios de puntos de distribución.

A continuación, habilite la función para un punto de distribución que recibe actualizaciones del Servidor de administración.

La función está activada en la configuración de directivas del Agente de red y, si los puntos de distribución se asignan manualmente y si desea anular la configuración de directivas, en la sección **Puntos de distribución** de las propiedades del Servidor de administración.

Para verificar que la función de descarga de archivos diff se habilite correctamente, puede medir el tráfico interno antes y después de realizar estos pasos.

# Crear la tarea para descargar actualizaciones en el repositorio del Servidor de administración

La tarea *Descargar actualizaciones en el repositorio del Servidor de administración* es creada automáticamente por el Asistente de inicio rápido de Kaspersky Security Center. No es posible crear más de una tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. Por lo tanto, para crear una tarea de este tipo, primero debe asegurarse de que no exista una tarea *Descargar actualizaciones en el repositorio del Servidor de administración* en la lista de tareas del Servidor de administración.

*Para crear una tarea "Descargar actualizaciones en el repositorio del Servidor de administración":*

1. En el árbol de la consola, seleccione la carpeta **Tareas**.
2. Realice una de las siguientes acciones para comenzar a crear la tarea:
   - En el árbol de la consola, abra el menú contextual de la carpeta **Tareas** y seleccione **Nuevo** → **Tarea**.
   - En el espacio de trabajo de la carpeta **Tareas**, haga clic en el botón **Crear una tarea**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.
3. En la página **Seleccione el tipo de tarea** del asistente, seleccione **Descargar actualizaciones en el repositorio del Servidor de administración**.

4. En la página **Configuración** del asistente, defina los siguientes ajustes para la tarea:

- Orígenes de actualizaciones

  Los siguientes recursos pueden utilizarse como orígenes de actualizaciones para el Servidor de administración:

  - Servidores de actualizaciones de Kaspersky

    Servidores HTTP(S) de Kaspersky desde los que las aplicaciones de Kaspersky descargan actualizaciones para sus bases de datos y módulos de software. De forma predeterminada, el Servidor de administración utiliza el protocolo HTTPS para comunicarse con los servidores de actualizaciones de Kaspersky y descargar las actualizaciones. Si lo desea, puede hacer que el Servidor de administración utilice el protocolo HTTP en lugar del protocolo HTTPS.

    Esta es la opción seleccionada por defecto.

  - Servidor de administración principal

    Este recurso se aplica a las tareas creadas para un Servidor de administración secundario o virtual.

  - Carpeta local o de red

    Una carpeta local o de red con las últimas actualizaciones. La carpeta de red puede ser un servidor FTP o HTTP, o un recurso compartido SMB. Si el acceso a la carpeta requiere autenticación, solo puede usarse el protocolo SMB. La carpeta local debe ser una carpeta del dispositivo en el que se encuentra instalado el Servidor de administración.

    > El servidor FTP/HTTP o la carpeta de red utilizada por un origen de actualizaciones debe contener una estructura de carpetas (con actualizaciones) que coincida con la estructura que se crea al usar los servidores de actualizaciones de Kaspersky.

- **Otras opciones**:

  - Forzar actualización de los servidores de administración secundarios

    Si esta opción está habilitada, el Servidor de administración iniciará las tareas de actualización en los servidores de administración secundarios en cuanto se descarguen nuevas actualizaciones. Las tareas de actualización se inician utilizando el origen de actualización configurado en las propiedades de la tarea en los Servidores de administración secundarios.

    Si esta opción no está habilitada, las tareas de actualización se iniciarán en los Servidores de administración secundarios siguiendo lo que indiquen sus programaciones.

    Esta opción está deshabilitada de forma predeterminada.

  - Copiar actualizaciones descargadas a carpetas adicionales

Una vez que el Servidor de administración recibe actualizaciones, las copiará a las carpetas especificadas. Utilice esta opción si desea controlar manualmente la distribución de actualizaciones en la red.

Podría utilizar esta opción en, por ejemplo, la siguiente situación: la red de su organización está formada por varias subredes independientes. Los dispositivos de cada subred no tienen acceso a las demás subredes. Sin embargo, los dispositivos de todas las subredes tienen acceso a una misma carpeta compartida. En un caso así, puede hacer que el Servidor de administración de una subred descargue las actualizaciones de los servidores de actualizaciones de Kaspersky, habilitar esta opción y definir esa carpeta compartida como destino. Luego, defina esa carpeta como origen de actualizaciones en las tareas "Descargar actualizaciones en el repositorio del Servidor de administración" de los demás servidores de administración.

Si selecciona copiar las actualizaciones descargadas a una carpeta local, debe especificar una carpeta en el dispositivo que tiene el Servidor de administración instalado. La ruta a la carpeta depende del sistema operativo del dispositivo. Dado que la carpeta local se encuentra en el Servidor de administración basado en Linux, debe especificar la ruta POSIX, por ejemplo: /path/to/dir.

Cuando selecciona una carpeta de red que se encuentra en el Servidor de administración basado en Linux, debe montar la carpeta para garantizar el acceso a la carpeta de red con anticipación desde el dispositivo que tiene el Servidor de administración. El acceso a la carpeta se realiza mediante el protocolo de SMB.

Esta opción está deshabilitada de forma predeterminada.

- **No forzar la actualización de los dispositivos y de los servidores de administración secundarios si la copia no se ha completado**

  Las tareas para descargas actualizaciones en los dispositivos cliente y en los servidores de administración secundarios no se iniciarán hasta que las actualizaciones hayan terminado de copiarse de la carpeta de actualización principal a las carpetas de actualización adicionales.

  Debe habilitar esta opción si sus dispositivos cliente y sus servidores de administración secundarios obtienen sus actualizaciones de carpetas de red adicionales.

  Esta opción está deshabilitada de forma predeterminada.

- **Descargar las actualizaciones usando el esquema antiguo**

A partir de la versión 14, Kaspersky Security Center utiliza el nuevo esquema al descargar actualizaciones para bases de datos y módulos de software. Para que la aplicación descargue las actualizaciones utilizando el nuevo esquema, el origen de actualizaciones debe contener archivos de actualización con metadatos que sean compatibles con el nuevo esquema. Si el origen de actualizaciones elegido contiene archivos de actualización con metadatos que solo son compatibles con el esquema anterior, habilite la opción **Descargar las actualizaciones usando el esquema antiguo**. De lo contrario, la tarea de descarga de actualizaciones no podrá completarse.

Habilite esta opción si, por ejemplo, ha seleccionado una carpeta local o de red como origen de actualizaciones y los archivos de actualización de dicha carpeta fueron descargados por alguna de las siguientes aplicaciones:

- Kaspersky Update Utility

  Esta utilidad descarga actualizaciones utilizando el esquema antiguo.

- Kaspersky Security Center 13.2 o una versión anterior

  Suponga, por ejemplo, que uno de sus servidores de administración no tiene conexión a Internet. En ese caso, podría utilizar un segundo Servidor de administración (que tenga conexión a Internet) para descargar las actualizaciones. Luego, podría colocar los archivos descargados en una carpeta local o de red que el primer servidor de administración pueda usar como origen de actualizaciones. Si el segundo Servidor de administración es de versión 13.2 o anterior, habilite la opción **Descargar las actualizaciones usando el esquema antiguo** en la tarea para el primer Servidor de administración.

Esta opción está deshabilitada de forma predeterminada.

5. En la página **Configurar programación de tarea** del asistente, puede crear una programación para el inicio de la tarea. De ser necesario, configure los siguientes ajustes:

- Inicio programado:

  Seleccione y configure la programación según la cual se ejecutará la tarea.

  - Cada N horas

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

    De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

  - Cada N días

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

    De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

  - Cada N semanas

    La tarea se ejecutará periódicamente, a intervalos regulares, en el día de la semana y a la hora que especifique. Cada ejecución estará separada de la anterior por el número de semanas que indique.

    Por defecto, la tarea se ejecutará cada lunes a la hora actual del sistema.

  - Cada N minutos

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

    De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

  - Diario (no compatible con horario de verano)

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta programación no tiene en cuenta los cambios de horario estacionales. La hora de inicio de la tarea se mantendrá sin cambios incluso si el reloj se atrasa o se adelanta una hora debido al horario de verano.

    No recomendamos usar esta programación. Se la ofrece para mantener la compatibilidad con versiones anteriores de Kaspersky Security Center.

    De forma predeterminada, la tarea se iniciará todos los días a la hora actual del sistema.

  - Semanal

La tarea se ejecutará cada semana en el día y a la hora que indique.

- **Por días de la semana**

  La tarea se ejecutará periódicamente en los días de la semana y a la hora que indique.

  De manera predeterminada, la tarea se ejecutará todos los viernes a las 18:00:00.

- **Mensual**

  La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

  Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

  Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

- **Manual**

  La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

  Esta opción está seleccionada de forma predeterminada.

- **Cada mes en los días especificados de semanas seleccionadas**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  Por defecto, la hora de inicio es a las 18:00 y no se selecciona ningún día del mes.

  Tenga en cuenta que no selecciona una fecha específica en el mes, ni el número de la semana (primera, segunda semana del mes), sino el número de secuencia del día de la semana dentro de un mes. Por ejemplo, si coloca el cursor en la celda **Ma** de la **Primero** fila, significa que la tarea se ejecutará el primer martes de cada mes nuevo.

  Puede seleccionar varios días de la semana.

- **Ante brotes de virus**

  La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para defensa del perímetro
  - Antivirus para sistemas de correo

  Por defecto, están seleccionados todos los tipos de aplicaciones.

  En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- **Al completarse otra tarea**

  La tarea actual se iniciará después de que se complete otra tarea. Esta opción solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

- **Ejecutar tareas no realizadas**

  Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

  Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

  Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

  Esta opción está deshabilitada de forma predeterminada.

- **Esperar un tiempo definido al azar antes de iniciar la tarea**

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

- **Limitar el tiempo de espera a esta cantidad de minutos**

Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

6. En la página **Defina el nombre de la tarea** del asistente, especifique el nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).

7. En la página **Finalizar la creación de la tarea** del asistente, haga clic en el botón **Finalizar** para cerrar el asistente.

   Para que la tarea se inicie en cuanto se cierre el asistente, marque la casilla **Ejecutar la tarea al finalizar el asistente**.

Una vez que se cierre el asistente, la tarea **Descargar actualizaciones en el repositorio del Servidor de administración** se agregará a la lista de tareas del Servidor de administración disponible en el espacio de trabajo.

Además de los ajustes configurados durante el proceso de creación, la tarea tiene otras propiedades que se pueden modificar.

Cuando el Servidor de administración realiza la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, se descargan actualizaciones para bases de datos y módulos de software del origen de actualizaciones. Los archivos descargados se guardan en la carpeta compartida del Servidor de administración. Si crea esta tarea para un grupo de administración, la misma se aplicará solamente a los agentes de red incluidos en el grupo de administración especificado.

Las actualizaciones se distribuyen a los dispositivos cliente y a los servidores de administración secundarios desde la carpeta compartida del Servidor de administración.

# Creación de la tarea Descargar actualizaciones en los repositorios de los puntos de distribución

Los puntos de distribución con macOS no pueden descargar actualizaciones de los servidores de actualizaciones de Kaspersky.

Si hay uno o más dispositivos con macOS en el alcance de la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*, la tarea terminará con el estado *Error* aunque se complete sin errores en todos los dispositivos con Windows.

Puede crear la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución* para un grupo de administración. Cuando la tarea se ejecute, afectará a los puntos de distribución que formen parte del grupo de administración seleccionado.

Puede usar esta tarea si, por ejemplo, su Servidor de administración no tiene acceso a Internet o si transmitir datos entre el Servidor de administración y los puntos de distribución es más costoso que hacerlo entre los puntos de distribución y los servidores de actualizaciones de Kaspersky. Si el punto de distribución se conecta a Internet mediante un servidor proxy, debe especificar la configuración correspondiente en la directiva del Agente de red.

*Para crear la tarea "Descargar actualizaciones en los repositorios de los puntos de distribución" para un grupo de administración seleccionado:*

1. En el árbol de la consola, seleccione la carpeta **Tareas**.

2. En el espacio de trabajo de esta carpeta, haga clic en el botón **Nueva tarea**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.

3. En la página **Seleccione el tipo de tarea** del Asistente, seleccione el nodo **Servidor de administración de Kaspersky Security Center**, expanda la carpeta **Avanzado** y seleccione la tarea **Descargar actualizaciones en los repositorios de los puntos de distribución**.

4. En la página **Configuración** del asistente, defina los siguientes ajustes para la tarea:

- Orígenes de actualizaciones

  Los siguientes recursos se pueden utilizar como orígenes de actualizaciones para el punto de distribución:

  - Servidores de actualizaciones de Kaspersky

    Servidores HTTP(S) de Kaspersky desde los que las aplicaciones de Kaspersky descargan actualizaciones para sus bases de datos y módulos de software.

    Esta opción está seleccionada de forma predeterminada.

  - Carpeta local o de red

    Una carpeta local o de red con las últimas actualizaciones. La carpeta de red puede ser un servidor FTP o HTTP, o un recurso compartido SMB. Si el acceso a la carpeta requiere autenticación, solo puede usarse el protocolo SMB. La carpeta local debe ser una carpeta del dispositivo en el que se encuentra instalado el Servidor de administración.

    El servidor FTP/HTTP o la carpeta de red utilizada por un origen de actualizaciones debe contener una estructura de carpetas (con actualizaciones) que coincida con la estructura que se crea al usar los servidores de actualizaciones de Kaspersky.

- Carpeta para almacenar actualizaciones

  La ruta a la carpeta especificada para almacenar las actualizaciones guardadas. Puede copiar la ruta de la carpeta especificada en el portapapeles. No puede cambiar la ruta a una carpeta específica para una tarea de grupo.

- Descargar las actualizaciones usando el esquema antiguo

A partir de la versión 14, Kaspersky Security Center utiliza el nuevo esquema al descargar actualizaciones para bases de datos y módulos de software. Para que la aplicación descargue las actualizaciones utilizando el nuevo esquema, el origen de actualizaciones debe contener archivos de actualización con metadatos que sean compatibles con el nuevo esquema. Si el origen de actualizaciones elegido contiene archivos de actualización con metadatos que solo son compatibles con el esquema anterior, habilite la opción **Descargar las actualizaciones usando el esquema antiguo**. De lo contrario, la tarea de descarga de actualizaciones no podrá completarse.

Habilite esta opción si, por ejemplo, seleccionó una carpeta local o de red como origen de actualizaciones y los archivos de actualización de dicha carpeta fueron descargados por alguna de las siguientes aplicaciones:

- Kaspersky Update Utility

  Esta utilidad descarga actualizaciones utilizando el esquema antiguo.

- Kaspersky Security Center 13.2 o una versión anterior

  Suponga, por ejemplo, que un punto de distribución está configurado para tomar las actualizaciones de una carpeta local o de red. En ese caso, puede utilizar un Servidor de administración que tenga conexión a Internet para descargar las actualizaciones y colocar los archivos descargados en la carpeta local del punto de distribución. Si el Servidor de administración es de versión 13.2 o anterior, habilite la opción **Descargar las actualizaciones usando el esquema antiguo** en la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*.

Esta opción está deshabilitada de forma predeterminada.

5. En la página **Seleccione un grupo de administración** del Asistente, haga clic en **Examinar** y seleccione el grupo de administración para el que se realizará la tarea.

6. En la página **Configurar programación de tarea** del asistente, puede crear una programación para el inicio de la tarea. De ser necesario, configure los siguientes ajustes:

- Inicio programado:

  Seleccione y configure la programación según la cual se ejecutará la tarea.

  - Cada N horas

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

    De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

  - Cada N días

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

    De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

  - Cada N semanas

    La tarea se ejecutará periódicamente, a intervalos regulares, en el día de la semana y a la hora que especifique. Cada ejecución estará separada de la anterior por el número de semanas que indique.

    Por defecto, la tarea se ejecutará cada lunes a la hora actual del sistema.

  - Cada N minutos

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

    De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

  - Diario (no compatible con horario de verano)

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta programación no tiene en cuenta los cambios de horario estacionales. La hora de inicio de la tarea se mantendrá sin cambios incluso si el reloj se atrasa o se adelanta una hora debido al horario de verano.

    No recomendamos usar esta programación. Se la ofrece para mantener la compatibilidad con versiones anteriores de Kaspersky Security Center.

    De forma predeterminada, la tarea se iniciará todos los días a la hora actual del sistema.

  - Semanal

La tarea se ejecutará cada semana en el día y a la hora que indique.

- **Por días de la semana**

  La tarea se ejecutará periódicamente en los días de la semana y a la hora que indique.

  De manera predeterminada, la tarea se ejecutará todos los viernes a las 18:00:00.

- **Mensual**

  La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

  Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

  Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

- **Manual**

  La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

  Esta opción está seleccionada de forma predeterminada.

- **Cada mes en los días especificados de semanas seleccionadas**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  Por defecto, la hora de inicio es a las 18:00 y no se selecciona ningún día del mes.

  Tenga en cuenta que no selecciona una fecha específica en el mes, ni el número de la semana (primera, segunda semana del mes), sino el número de secuencia del día de la semana dentro de un mes. Por ejemplo, si coloca el cursor en la celda **Ma** de la **Primero** fila, significa que la tarea se ejecutará el primer martes de cada mes nuevo.

  Puede seleccionar varios días de la semana.

- **Ante brotes de virus**

  La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para defensa del perímetro
  - Antivirus para sistemas de correo

  Por defecto, están seleccionados todos los tipos de aplicaciones.

  En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- **Al completarse otra tarea**

  La tarea actual se iniciará después de que se complete otra tarea. Esta opción solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

- **Ejecutar tareas no realizadas**

  Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

  Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

  Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

  Esta opción está deshabilitada de forma predeterminada.

- **Esperar un tiempo definido al azar antes de iniciar la tarea**

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

- **Limitar el tiempo de espera a esta cantidad de minutos**

Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

7. En la página **Defina el nombre de la tarea** del asistente, especifique el nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).

8. En la página **Finalizar la creación de la tarea** del asistente, haga clic en el botón **Finalizar** para cerrar el asistente.

   Para que la tarea se inicie en cuanto se cierre el asistente, marque la casilla **Ejecutar la tarea al finalizar el asistente**.

Una vez que el Asistente complete su operación, encontrará la tarea **Descargar actualizaciones en los repositorios de los puntos de distribución** en la lista de tareas del Agente de red asociadas al grupo de administración seleccionado y en el espacio de trabajo **Tareas** de la consola.

Además de los ajustes configurados durante el proceso de creación, la tarea tiene otras propiedades que se pueden modificar.

Cuando se ejecute la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*, se descargarán actualizaciones para bases de datos y módulos de software del origen de actualizaciones. Los archivos descargados se guardarán en la carpeta compartida. Las actualizaciones descargadas solo serán utilizadas por los puntos de distribución que formen parte del grupo de administración especificado y que no tengan una tarea de descarga de actualizaciones explícitamente definida para ellos.

En la ventana de propiedades del Servidor de administración, en el panel **Secciones**, seleccione **Puntos de distribución**. En las propiedades de cada punto de distribución, en la sección **Origen de actualizaciones**, puede elegir el origen de actualizaciones (**Recuperar desde el Servidor de administración** o **Utilizar la tarea para la descarga forzada de actualizaciones**). La opción **Recuperar desde el Servidor de administración** está seleccionada por defecto para puntos de distribución designados manual o automáticamente. Estos puntos de distribución usarán los resultados de la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*.

Las propiedades de cada punto de distribución determinan la carpeta de red configurada individualmente para ese punto de distribución. Los nombres de las carpetas pueden variar de un punto de distribución a otro. Por este motivo, no recomendamos cambiar la carpeta de red en las propiedades de una tarea creada para un grupo de dispositivos.

Puede cambiar la carpeta de red que contiene las actualizaciones en las propiedades de la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución* si está creando una tarea local para un dispositivo.

# Configuración de la tarea del Servidor de administración Descargar actualizaciones en el repositorio

*Para configurar la tarea del Servidor de administración Descargar actualizaciones en el repositorio:*

1. En el espacio de trabajo de la carpeta del árbol de la consola **Tareas**, seleccione **Descargar actualizaciones al repositorio del Servidor de administración** de la lista de tareas.

2. Abra la ventana de propiedades de la tarea de una de las siguientes formas:

   - Seleccione **Propiedades** en el menú contextual de la tarea.

   - Haga clic en el enlace **Configurar tarea** en el cuadro de información de la tarea seleccionada.

   Se abre la ventana de propiedades de la tarea del Servidor de administración *Descargar actualizaciones en el repositorio*. En esta ventana puede configurar cómo se descargarán las actualizaciones al repositorio del Servidor de administración.

# Comprobar actualizaciones descargadas

Antes de instalar actualizaciones en sus dispositivos administrados, puede comprobar que las mismas no tengan errores o problemas de funcionamiento. Dispone para ello de la tarea *Verificación de actualizaciones*. La tarea *Verificación de actualizaciones* se ejecuta automáticamente cuando se realiza la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. El Servidor de administración descarga las actualizaciones del origen, las guarda en el repositorio temporal y ejecuta la tarea *Verificación de actualizaciones*. Si la tarea se completa sin errores, las actualizaciones se copian del repositorio temporal a la carpeta compartida del Servidor de administración (<Carpeta de instalación de Kaspersky Security Center>\Share\Updates). De allí, se distribuyen a los dispositivos cliente que tienen el Servidor de administración como origen de actualizaciones.

Si, como resultado de la tarea *Verificación de actualizaciones*, se determina que las actualizaciones del repositorio temporal son incorrectas, o si la tarea *Verificación de actualizaciones* se completa con errores, las actualizaciones problemáticas no se copian a la carpeta compartida. El Servidor de administración guarda el conjunto de actualizaciones anterior. Además, las tareas que tienen el tipo de programación **Al descargar nuevas actualizaciones al repositorio** no se inician en ese momento. Dichas operaciones se llevarán a cabo en el siguiente inicio de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* si el análisis de las nuevas actualizaciones finaliza correctamente.

El conjunto de actualizaciones se considera inválido si una de las condiciones siguiente se cumple al menos en un dispositivo de prueba:

- Ocurrió un error de la tarea de actualización.

- El estado de protección en tiempo real de la aplicación de seguridad cambió después de haber aplicado las actualizaciones.

- Se detectó un objeto infectado mientras se ejecutaba la tarea de análisis a pedido.

- Se produjo un error en el tiempo de ejecución de la aplicación de Kaspersky.

Si estas condiciones no se cumplen en ninguno de los dispositivos de prueba, el conjunto de actualizaciones se considera válido y la tarea *Verificación de actualizaciones* se da por correctamente completada.

Antes de comenzar a crear la tarea *Verificación de actualizaciones*, complete estos pasos:

1. Cree un grupo de administración que contenga algunos dispositivos de prueba. El grupo se usará para verificar las actualizaciones.

   Recomendamos que los dispositivos del grupo tengan la protección más fiable posible y que su configuración de aplicaciones sea la más usual en la red. Con ello mejorará la fiabilidad de los análisis antivirus, aumentará la probabilidad de que se detecten virus y se reducirá la incidencia de falsos positivos. De encontrarse virus en los dispositivos de prueba, se considerará que la tarea *Verificación de actualizaciones* no se completó correctamente.

2. Cree las tareas *Actualización* y *Análisis antimalware* para una aplicación compatible con Kaspersky Security Center, como Kaspersky Endpoint Security para Windows o Kaspersky Security for Windows Server. Cuando cree las tareas *Actualización* y *Análisis antimalware*, seleccione el grupo de administración que contiene los dispositivos de prueba.

   La tarea *Verificación de actualizaciones* ejecuta las tareas *Actualización* y *Análisis antimalware* secuencialmente en los dispositivos de prueba para verificar que todas las actualizaciones sean válidas. Cuando cree la tarea *Verificación de actualizaciones*, deberá seleccionar las tareas *Actualización* y *Análisis antimalware* que se ejecutarán.

3. Cree la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*.

*Para que Kaspersky Security Center verifique las actualizaciones descargadas antes de distribuirlas a los dispositivos cliente:*

1. En el espacio de trabajo de la carpeta **Tareas**, seleccione la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* en la lista de tareas.

2. Abra la ventana de propiedades de la tarea de una de las siguientes formas:

   - Seleccione **Propiedades** en el menú contextual de la tarea.
   - Haga clic en el enlace **Configurar tarea** en el cuadro de información de la tarea seleccionada.

3. Si la tarea *Verificación de actualizaciones* ya existe, haga clic en el botón **Examinar**. En la ventana que se abre, seleccione la tarea *Verificación de actualizaciones* del grupo de administración con los dispositivos de prueba.

4. Si aún no creó la tarea *Verificación de actualizaciones*, haga clic en el botón **Crear**.

   Se inicia la tarea *Verificación de actualizaciones*. Siga las instrucciones del asistente.

5. Haga clic en **Aceptar** para cerrar la ventana de propiedades de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*.

La verificación de actualización automática está habilitada. Ahora puede ejecutar la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* y comenzará desde la verificación de actualizaciones.

# Configurar las directivas de prueba y tareas auxiliares

Cuando se crea una tarea *Verificación de actualizaciones*, el Servidor de administración genera directivas de prueba, tareas de actualización de grupo auxiliares y tareas de análisis a pedido.

> Las tareas de actualización de grupo auxiliares y tareas de análisis a pedido llevan tiempo. Estas tareas se llevan a cabo cuando se ejecuta la tarea *Verificación de actualizaciones*. La tarea *Verificación de actualizaciones* se realiza durante la ejecución de la tarea *Descargar actualizaciones en el repositorio*. La duración de la tarea *Descargar actualizaciones en el repositorio* incluye la actualización del grupo auxiliar y las tareas de análisis a pedido.

Puede cambiar la configuración de las directivas de prueba y tareas auxiliares.

*Para cambiar la configuración de una directiva de prueba o una tarea auxiliar:*

1. En el árbol de la consola, seleccione un grupo para el que se haya creado la tarea *Verificación de actualizaciones*.
2. En el espacio de trabajo del grupo, seleccione una de las siguientes pestañas:
   - **Directivas**, si desea editar la configuración de directivas de prueba.
   - **Tareas**, si desea cambiar la configuración de tarea auxiliar.
3. En la pestaña de espacio de trabajo, seleccione una directiva o tarea, a la que desee cambiarle la configuración.
4. Abra la ventana de propiedades de la directiva (tarea) de una de las siguientes formas:
   - Seleccione **Propiedades** en el menú contextual de la directiva (tarea).
   - Haga clic en el enlace **Configurar directiva** (**Configurar tarea**) en el cuadro de información de la directiva (tarea) seleccionada.

Para verificar correctamente las actualizaciones, configure siguientes restricciones en la modificación de las directivas de prueba y tareas auxiliares:

- En la configuración de tarea auxiliar:
  - Guarde todas las tareas con los niveles de importancia **Evento crítico** y **Error funcional** en el Servidor de administración. Usando los eventos de estos tipos, el Servidor de administración analiza la operación de aplicaciones.
  - Usar el Servidor de administración como el origen de actualizaciones.
  - Especifique el tipo de programación de tarea: **Manual**.
- En los parámetros de las directivas de prueba:
  - Deshabilite las tecnologías de aceleración de escaneo iChecker y iSwift (**Protección básica contra amenazas → Protección contra archivos peligrosos → Configuración → Adicional → Tecnologías de escaneo**).
  - Seleccione acciones sobre los objetos infectados: **Desinfectar; eliminar si falla la desinfección** / **Desinfectar; bloquear si falla la desinfección** / **Bloquear**. (**Protección básica contra amenazas → Protección contra archivos peligrosos → Acción al detectar amenazas**).
- En la configuración de las directivas de prueba y tareas auxiliares:

  Si después de la instalación de actualizaciones para módulos de software se requiere un reinicio del dispositivo, es necesario que lo reinicie inmediatamente. Si no se reinicia el dispositivo, no es posible probar este tipo de actualizaciones. Para algunas aplicaciones, la instalación de actualizaciones que requieren el reinicio puede ser prohibida o configurada para solicitar al usuario la confirmación primero. Estas restricciones deben deshabilitarse en la configuración de las directivas de prueba y tareas auxiliares.

# Ver actualizaciones descargadas

*Para ver la lista de actualizaciones descargadas,*

En el árbol de la consola, en la carpeta **Repositorios**, seleccione la subcarpeta **Actualizaciones para bases de datos y módulos de software de Kaspersky**.

El espacio de trabajo de la carpeta **Actualizaciones para bases de datos y módulos de software de Kaspersky** muestra la lista de actualizaciones guardadas en el Servidor de administración.

# Instalación automática de actualizaciones de Kaspersky Endpoint Security en los dispositivos

Puede configurar las actualizaciones automáticas de las bases de datos y los módulos de software de Kaspersky Endpoint Security en los dispositivos cliente.

*Para configurar la descarga e instalación automáticas de actualizaciones de Kaspersky Endpoint Security en los dispositivos:*

1. En el árbol de la consola, seleccione la carpeta **Tareas**.
2. Cree una tarea **Actualizar** de una de las siguientes formas:
   - Seleccione **Nuevo → Tarea** en el menú contextual de la carpeta **Tareas** en el árbol de la consola.
   - Haga clic en el botón **Nueva tarea** en el espacio de trabajo de la carpeta **Tareas**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.
3. En la página **Seleccione el tipo de tarea** del Asistente, seleccione **Kaspersky Endpoint Security** como tipo de tarea y, a continuación, seleccione **Actualizar** como subtipo de tarea.
4. Siga el resto de instrucciones del asistente.

   Una vez que finalice el Asistente, se crea una tarea de actualización para Kaspersky Endpoint Security. La tarea nueva se muestra en la lista de tareas del espacio de trabajo de la carpeta **Tareas**.
5. En el espacio de trabajo de la carpeta **Tareas**, seleccione una tarea de actualización que haya creado.
6. En el menú contextual de la tarea, seleccione **Propiedades**.
7. En la ventana de propiedades de la tarea que se abre, en el panel **Secciones**, seleccione **Opciones**.

   En la sección **Opciones** puede configurar los ajustes de la tarea de actualización en el modo local o móvil:
   - **Configuración de actualización para el modo local**: la conexión se establece entre el dispositivo y el Servidor de administración.
   - **Configuración de actualizaciones para el modo móvil**: No se establece ninguna conexión entre Kaspersky Security Center y el dispositivo (por ejemplo, cuando el dispositivo no está conectado a Internet).
8. Haga clic en el botón **Configuración** para seleccionar el origen de la actualización.
9. Seleccione la opción **Descargar actualizaciones de módulos de la aplicación** para descargar e instalar las actualizaciones de módulos de software junto con las bases de datos de la aplicación.

   Si se selecciona esta casilla, Kaspersky Endpoint Security notifica al usuario acerca de las actualizaciones de módulos de software disponibles y las incluye en el paquete de actualización mientras ejecuta la tarea de actualización. Configure el uso de los módulos de actualización:
   - **Instalar actualizaciones críticas y aprobadas**. Si hay actualizaciones disponibles para los módulos de software, Kaspersky Endpoint Security instala automáticamente las que tienen estado *Crítico*; las actualizaciones restantes se instalarán después de que usted las apruebe.
   - **Instalar las actualizaciones aprobadas únicamente**. Si hay actualizaciones disponibles para los módulos de software y se aprueba su instalación, Kaspersky Endpoint Security las instala de manera local mediante la interfaz de la aplicación o mediante Kaspersky Security Center.

   Para actualizar los módulos de software, podría resultar necesario leer y aceptar los términos del contrato de licencia y de la política de privacidad. Cuando este sea el caso, la aplicación esperará a que el usuario acepte los términos de estos documentos y luego instalará las actualizaciones.

10. Active la opción **Copiar actualizaciones a carpeta** para que la aplicación guarde las actualizaciones descargadas en una carpeta y, a continuación, haga clic en el botón **Examinar** para especificar la carpeta.

11. Haga clic en **Aceptar**.

Cuando la tarea **Actualizar** está en ejecución, la aplicación envía solicitudes a los servidores de actualizaciones de Kaspersky.

Algunas actualizaciones requieren que estén instaladas las últimas versiones de los complementos de administración.

# Modelo de descarga de actualizaciones sin conexión

A veces, los Agentes de red de los dispositivos administrados no se pueden conectar al Servidor de administración para recibir actualizaciones. Por ejemplo, el Agente de red puede estar instalado en un equipo portátil que a veces no tiene conexión a Internet ni acceso a la red local. También es posible que el administrador limite el tiempo de conexión de los dispositivos cliente a la red. En estos casos, los dispositivos con el Agente de red instalado no pueden recibir actualizaciones del Servidor de administración según la programación existente. Si configuró la actualización de aplicaciones administradas (como, por ejemplo, Kaspersky Endpoint Security) mediante el Agente de red, deberá estar conectado al Servidor de administración para recibir cada actualización. Cuando no hay una conexión establecida entre el Agente de red y el Servidor de administración, es imposible llevar a cabo la actualización. Puede configurar la conexión entre el Agente de red y el Servidor de administración de modo que el Agente de red se conecte al Servidor de administración en intervalos de tiempo especificados. En el peor de los casos, si los intervalos de conexión especificados coinciden con periodos en los que la conexión no está disponible, las bases de datos nunca se actualizarán. Además, pueden producirse problemas cuando varias aplicaciones administradas intentan acceder al Servidor de administración de manera simultánea para recibir actualizaciones. En este caso, es posible que el Servidor de administración deje de responder a las solicitudes (algo similar a un ataque DDoS).

Para evitar problemas como los descritos, en Kaspersky Security Center se ha implementado un modelo de descarga de actualizaciones y módulos de aplicaciones administradas que no requiere conexión. Este modelo proporciona un mecanismo para la distribución de actualizaciones, sin tener en cuenta problemas temporales causados por la inaccesibilidad de canales de comunicación del Servidor de administración. El modelo también reduce la carga en el Servidor de administración.

## Cómo funciona el modelo de descarga de actualizaciones sin conexión

Cuando el Servidor de administración recibe actualizaciones, notifica al Agente de red (en los dispositivos donde está instalado) las actualizaciones que serán necesarias para las aplicaciones administradas. Cuando el Agente de red recibe la información sobre las actualizaciones, descarga por anticipado los archivos relevantes desde el Servidor de administración. En la primera conexión con un Agente de red, el Servidor de administración inicia una descarga de actualizaciones. Después de que Agente de red descarga todas las actualizaciones a un dispositivo cliente, las actualizaciones quedan disponibles para las aplicaciones en ese dispositivo.

Cuando una aplicación administrada de un dispositivo cliente intenta acceder al Agente de red para descargar actualizaciones, el Agente de red comprueba si tiene todas las actualizaciones necesarias. Si las actualizaciones se reciben desde el Servidor de administración no más de 25 horas antes de que la aplicación administrada las solicite, el Agente de red no se conecta al Servidor de administración, sino que proporciona actualizaciones desde el caché local a la aplicación administrada. Es posible que la conexión con el Servidor de administración no se establezca cuando el Agente de red proporciona actualizaciones para las aplicaciones en los dispositivos cliente, pero no se requiere conexión para la actualización.

Para distribuir la carga en el Servidor de administración, el Agente de red se conecta al Servidor de administración y descargan actualizaciones en un orden aleatorio durante el intervalo de tiempo especificado por el Servidor de administración. Este intervalo de tiempo depende del número de dispositivos con el Agente de red instalado que descargan actualizaciones y del tamaño de dichas actualizaciones. Para reducir la carga del Servidor de administración, el Agente de red puede funcionar como punto de distribución.

Si el modelo de descarga de actualizaciones sin conexión está desactivado, las actualizaciones se distribuyen de acuerdo con el programa de la tarea de descarga de actualizaciones.

De manera predeterminada, el modelo de descarga sin conexión está habilitado.

El modelo sin conexión solo se usa con los dispositivos administrados en los cuales la tarea para que las aplicaciones administradas descarguen actualizaciones tiene seleccionado **Al descargar nuevas actualizaciones al repositorio** como tipo de planificación. Para los demás dispositivos administrados, se usa el esquema estándar para recibir actualizaciones desde el Servidor de administración en modo de tiempo real.

Recomendamos que desactive el modelo de descarga de actualizaciones sin conexión usando la configuración de las directivas del Agente de red de los grupos de administración correspondientes en estos casos: si las aplicaciones administradas tienen configurada la recuperación de actualizaciones no desde el Servidor de administración, sino desde los servidores de Kaspersky o desde una carpeta de la red, y si la tarea de descarga de actualizaciones tiene la opción **Al descargar nuevas actualizaciones al repositorio** seleccionada como tipo de planificación.

# Habilitación y deshabilitación del modelo de descarga de actualizaciones sin conexión

Recomendamos que evite deshabilitar el modelo de descarga de actualizaciones sin conexión. Deshabilitarlo puede causar fallos en la entrega de actualización a dispositivos. Sin embargo, en ciertos casos, un especialista del Servicio de soporte técnico de Kaspersky puede recomendar que desactive la casilla **Descargar actualizaciones y bases de datos antivirus del Servidor de administración con anticipación**. En este caso, tendrá que asegurarse de que la tarea para recibir actualizaciones para aplicaciones de Kaspersky esté configurada.

*Para habilitar o deshabilitar el modelo de descarga de actualizaciones sin conexión para un grupo de administración:*

1. En el árbol de la consola, seleccione el grupo de administración para el cual desee habilitar el modelo de descarga de actualizaciones sin conexión.
2. En el espacio de trabajo del grupo, abra la pestaña **Directivas**.
3. En la pestaña **Directivas**, seleccione la directiva de Agente de red.
4. En el menú contextual de la directiva, seleccione **Propiedades**.

   Abra la ventana Propiedades de la directiva del Agente de red.
5. En la ventana de propiedades de la directiva, seleccione la sección **Administrar parches y actualizaciones**.
6. Marque o desmarque la casilla **Descargar actualizaciones y bases de datos antivirus del Servidor de administración con anticipación (recomendado)** para habilitar o deshabilitar, respectivamente, el modelo de descarga de actualizaciones sin conexión.

   De manera predeterminada, el modelo de descarga sin conexión está habilitado.

El modelo de descarga de actualizaciones sin conexión se habilitará o se deshabilitará.

# Actualización automática y parches para componentes de Kaspersky Security Center

De forma predeterminada, cualquier actualización y parche que se haya descargado se instala automáticamente para los siguientes componentes de la aplicación:

- Agente de red para Windows
- Consola de administración
- Servidor de MDM para iOS

La actualización automática y la aplicación de parches para los componentes de Kaspersky Security Center están disponibles solo para dispositivos que ejecutan Windows. Puede deshabilitar la actualización automática y los parches para estos componentes. En este caso, cualquier actualización y parche que se haya descargado se instalarán únicamente después de que cambie su estado a *Aprobado*. Las actualizaciones y los parches con el estado *Sin definir* no se instalarán.

# Habilitación y deshabilitación de actualizaciones automáticas y parches para componentes de Kaspersky Security Center

La instalación automática de actualizaciones y parches para componentes de Kaspersky Security Center está habilitada de forma predeterminada durante la instalación del Agente de red en el dispositivo. Puede deshabilitarla durante la instalación del Agente de red o más adelante usando una directiva.

*Para deshabilitar la actualización automática y los parches para componentes de Kaspersky Security Center durante instalación local del Agente de red en un dispositivo, realice lo siguiente:*

1. Inicie la instalación local del Agente de red en el dispositivo.
2. En el paso **Configuración avanzada**, desactive la casilla **Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes**.
3. Siga las instrucciones del asistente.

Se instalará el Agente de red con la actualización automática y los parches para componentes de Kaspersky Security Center deshabilitados en el dispositivo. Si desea habilitar la autoinstalación de actualizaciones y parches más adelante, podrá hacerlo a través de una directiva.

*Para deshabilitar la actualización automática y los parches para componentes de Kaspersky Security Center durante la instalación del Agente de red en el dispositivo mediante un paquete de instalación, realice lo siguiente:*

1. En el árbol de consola, seleccione la carpeta **Instalación remota → Paquetes de instalación**.
2. En el menú contextual del paquete **Agente de red de Kaspersky Security Center <número de versión>**, seleccione **Propiedades**.
3. En las propiedades del paquete de instalación, en la sección **Configuración** borre la casilla de verificación **Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes**.

Se instalará el Agente de red con la actualización automática y los parches para componentes de Kaspersky Security Center deshabilitados de este paquete. Si desea habilitar la autoinstalación de actualizaciones y parches más adelante, podrá hacerlo a través de una directiva.

Si esta casilla se seleccionó (o se desactivó) durante la instalación del Agente de red en el dispositivo, puede habilitar posteriormente (o deshabilitar) la actualización automática usando la directiva del Agente de red.

*Para habilitar o deshabilitar la actualización automática y los parches para componentes de Kaspersky Security Center usando la directiva del Agente de red, realice lo siguiente:*

1. En el árbol de consola, seleccione el grupo de administración para el que desea habilitar o deshabilitar la actualización automática y los parches.
2. En el espacio de trabajo del grupo, abra la pestaña **Directivas**.
3. En la pestaña **Directivas**, seleccione la directiva de Agente de red.
4. En el menú contextual de la directiva, seleccione **Propiedades**.

   Abra la ventana Propiedades de la directiva del Agente de red.
5. En la ventana de propiedades de la directiva, seleccione la sección **Administrar parches y actualizaciones**.
6. Seleccione o borre la casilla de verificación **Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes** para habilitar o deshabilitar, respectivamente, actualizaciones y parches automáticos.
7. Configure el bloqueo para esta casilla.

La directiva se aplicará a los dispositivos seleccionados y la actualización automática y los parches para los componentes de Kaspersky Security Center se habilitarán (o se deshabilitarán) en estos dispositivos.

# Distribución automática de las actualizaciones

Kaspersky Security Center permite la distribución e instalación automática de actualizaciones en dispositivos cliente y Servidores de administración secundarios.

## Distribución automática de actualizaciones a dispositivos cliente

*Para distribuir las actualizaciones de la aplicación seleccionada a dispositivos cliente inmediata y automáticamente después de la descarga en el repositorio del Servidor de administración:*

1. Conéctese al Servidor de administración que administra los dispositivos cliente.
2. Utilice uno de estos métodos para crear una tarea de distribución de actualizaciones para los dispositivos cliente seleccionados:
   - Si necesita distribuir actualizaciones en dispositivos cliente que pertenecen al grupo de administración seleccionado, cree una tarea para el grupo seleccionado.
   - Si desea distribuir actualizaciones en dispositivos cliente que pertenecen a diferentes grupos de administración o no pertenecen a ninguno, cree una tarea para dispositivos específicos.

   Se inicia el Asistente para crear nueva tarea. Siga las instrucciones y realice las siguientes acciones:

   a. En la ventana del asistente **Tipo de tarea**, en el nodo de la aplicación requerida seleccione la tarea de despliegue de actualizaciones.

      El nombre de la tarea de distribución de actualizaciones que se muestra en la ventana **Tipo de tarea** depende de la aplicación para la cual creó esta tarea. Para obtener información detallada sobre los nombres de tareas de actualización para las aplicaciones de Kaspersky seleccionadas, consulte las guías correspondientes.

   b. En la ventana del asistente **Programación**, en el campo **Inicio programado**, seleccione **Al descargar nuevas actualizaciones al repositorio**.

   La tarea de distribución de actualizaciones creada se iniciará para los dispositivos seleccionados cada vez que se descargan actualizaciones en el repositorio del Servidor de administración.

Si una tarea de distribución de actualizaciones para la aplicación requerida se crea para los dispositivos seleccionados, para distribuir automáticamente actualizaciones a dispositivos cliente, en la ventana de propiedades de la tarea en la sección **Programación**, seleccione la opción **Al descargar nuevas actualizaciones al repositorio** como opción de inicio en el campo **Inicio programado**.

## Distribución automática de actualizaciones a Servidores de administración secundarios

*Para distribuir las actualizaciones de la aplicación seleccionada en los Servidores de administración secundarios inmediatamente después de la descarga de las actualizaciones en el repositorio del Servidor de administración principal:*

1. En el árbol de consola, en el nodo del Servidor de administración principal, seleccione la carpeta **Tareas**.
2. En la lista de tareas del espacio de trabajo, seleccione la tarea del Servidor de administración Descargar actualizaciones en el repositorio.

3. Abra la sección **Configuración** de la tarea seleccionada de una de las siguientes formas:

   - Seleccione **Propiedades** en el menú contextual de la tarea.
   - Haga clic en el vínculo **Modificar configuración** en el cuadro de información de la tarea seleccionada.

4. En la sección **Configuración** de la ventana Propiedades de la tarea, seleccione la subsección **Otras opciones** y haga clic en el enlace **Configurar**.

5. En la ventana **Otras opciones** que se abre, seleccione la casilla **Forzar actualización en los Servidores de administración secundarios**.

6. En la configuración de la tarea de descarga de actualizaciones del Servidor de administración, en la pestaña **Configuración** de la ventana Propiedades de la tarea, seleccione la casilla **Forzar actualización en los Servidores de administración secundarios**.

Una vez que el Servidor de administración principal recupere las actualizaciones, las tareas de descarga de actualizaciones se iniciarán automáticamente en los Servidores de administración secundarios sin importar su programación.

El Servidor de administración principal realiza la actualización de las bases de datos antivirus de acuerdo con las aplicaciones instaladas en los Servidores de administración secundarios. No es necesario instalar complementos adicionales ni crear paquetes de instalación en el Servidor de administración principal.

## Asignar puntos de distribución automáticamente

Recomendamos que asigne puntos de distribución automáticamente. Kaspersky Security Center seleccionará por sí mismo qué dispositivos deben tener asignados puntos de distribución.

*Para asignar puntos de distribución automáticamente:*

1. Abra la ventana principal de la aplicación.

2. En el árbol de la consola, seleccione el nodo con el nombre del Servidor de administración para el que desea asignar puntos de distribución automáticamente.

3. En el menú contextual del Servidor de administración, haga clic en **Propiedades**.

4. En la ventana de propiedades del Servidor de administración, en el panel **Secciones**, seleccione **Puntos de distribución**.

5. En la parte derecha de la ventana, seleccione la opción **Asignar puntos de distribución automáticamente**.

   Si la asignación automática de dispositivos como puntos de distribución está habilitada, no puede configurar los puntos de distribución manualmente ni editar la lista de puntos de distribución.

6. Haga clic en **Aceptar**.

El Servidor de administración asigna y configura los puntos de distribución automáticamente.

# Asignación manual de un punto de distribución a un dispositivo

Kaspersky Security Center permite asignar dispositivos para que actúen como puntos de distribución.

Recomendamos que asigne puntos de distribución automáticamente. En este caso, Kaspersky Security Center seleccionará por sí mismo qué dispositivos deben tener asignados puntos de distribución. Sin embargo, si tiene que optar por no asignar puntos de distribución automáticamente por cualquier motivo (por ejemplo, si desea utilizar servidores asignados exclusivamente), puede asignar puntos de distribución manualmente después de calcular su número y configuración.

Los dispositivos designados como puntos de distribución deben protegerse contra el acceso no autorizado por medios virtuales y físicos.

*Para designar manualmente un dispositivo como punto de distribución:*

1. En el árbol de consola, haga clic el nodo del **Servidor de administración**.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
3. En la ventana Propiedades del Servidor de administración, seleccione la sección **Puntos de distribución** y haga clic en el botón **Agregar**. Este botón está disponible si ha sido seleccionado **Asignar puntos de distribución manualmente**.

   Se abre la ventana **Agregar un punto de distribución**.
4. En la ventana **Agregar un punto de distribución**, realice las siguientes acciones:

   a. Seleccione un dispositivo que actuará como punto de distribución (seleccione uno en un grupo de administración o especifique la dirección IP de un dispositivo). Al seleccionar un dispositivo, tenga en cuenta las características de funcionamiento de los puntos de distribución y los requisitos establecidos para el dispositivo que actúa como punto de distribución.

   b. Indique los dispositivos específicos a los que el punto de distribución distribuirá las actualizaciones. Puede especificar un grupo de administración o una descripción de ubicación de red.
5. Haga clic en **Aceptar**.

   El punto de distribución agregado aparecerá en la lista de puntos de distribución, en la sección **Puntos de distribución**.

6. Seleccione el nuevo punto de distribución añadido en la lista y haga clic en el botón **Propiedades** para abrir la ventana de propiedades.

7. En la ventana de propiedades, configure los ajustes del punto de distribución:

   - La sección **General** contiene la configuración de interacción entre el punto de distribución y los dispositivos cliente.

     - **Puerto SSL**

       El número del puerto SSL que se usará para establecer una conexión cifrada con SSL entre el punto de distribución y los dispositivos cliente.

       De manera predeterminada, se utiliza el puerto 13000.

     - **Utilizar multidifusión**

       Si habilita esta opción, se utilizará la multidifusión IP para distribuir automáticamente los paquetes de instalación a los dispositivos cliente del grupo.

       Cuando necesite instalar una aplicación en un grupo de dispositivos cliente utilizando un paquete de instalación, la multidifusión IP ayudará a que el proceso se complete más rápidamente. Sin embargo, cuando se necesita instalar una aplicación en un único dispositivo cliente, la multidifusión hace que el tiempo de instalación aumente.

     - **Dirección de multidifusión IP**

       La dirección IP que se utilizará para la multidifusión. Puede usar cualquier dirección IP del intervalo 224.0.0.0-239.255.255.255

       De manera predeterminada, Kaspersky Security Center asignará automáticamente una dirección de multidifusión IP única tomada de este intervalo.

     - **Número de puerto multidifusión IP**

       Número del puerto que se usará para la multidifusión IP.

       El puerto por defecto es el 15001. De forma predeterminada, si el dispositivo que tiene instalado el Servidor de administración es, además, el punto de distribución designado, se usará el puerto 13001 para las conexiones SSL.

     - **Desplegar actualizaciones**

Las actualizaciones se distribuirán a los dispositivos administrados desde las siguientes fuentes:

- si deja esta opción habilitada: el presente punto de distribución;
- si deshabilita esta opción: otros puntos de distribución, el Servidor de administración o los servidores de actualizaciones de Kaspersky.

Si utiliza puntos de distribución para distribuir las actualizaciones, reducirá el número de descargas y verá una merma en el volumen de tráfico. Además, al distribuir la carga entre los puntos de distribución, también logrará aminorar la carga del Servidor de administración. Puede calcular cuántos puntos de distribución necesitará en su red para reducir los volúmenes de tráfico y de carga.

Si deshabilita esta opción, el número de descargas de actualizaciones y la carga del Servidor de administración podrían aumentar. Esta opción está activada de forma predeterminada.

- **Desplegar paquetes de instalación**

  Los paquetes de instalación se distribuirán a los dispositivos administrados desde las siguientes fuentes:

  - si deja esta opción habilitada: el presente punto de distribución;
  - si deshabilita esta opción: otros puntos de distribución, el Servidor de administración o los servidores de actualizaciones de Kaspersky.

  Si utiliza puntos de distribución para desplegar los paquetes de instalación, reducirá el número de descargas y verá una merma en el volumen de tráfico. Además, al distribuir la carga entre los puntos de distribución, también logrará aminorar la carga del Servidor de administración. Puede calcular cuántos puntos de distribución necesitará en su red para reducir los volúmenes de tráfico y de carga.

  Si deshabilita esta opción, el número de descargas de paquetes de instalación y la carga del Servidor de administración podrían aumentar. Esta opción está activada de forma predeterminada.

- **Use este punto de distribución como servidor push**

  En Kaspersky Security Center, un punto de distribución puede funcionar como servidor push para los dispositivos administrados a través del protocolo móvil. Por ejemplo, se debe habilitar un servidor push si quiere poder forzar la sincronización de los dispositivos KasperskyOS con el Servidor de administración. Un servidor push tiene el mismo alcance de los dispositivos administrados que el punto de distribución en el que se habilitar el servidor push. Si tiene varios puntos de distribución asignados para el mismo grupo de administración, puede habilitar el servidor push en cada uno de los puntos de distribución. En este caso, el Servidor de administración equilibra la carga entre los puntos de distribución.

  Si administra los dispositivos con KasperskyOS instalado, o tiene pensado hacerlo, debe utilizar un punto de distribución como servidor push. También puede utilizar un punto de distribución como servidor push si desea enviar notificaciones push a los dispositivos cliente.

- **Puerto del servidor push**

  El puerto del punto de distribución que los dispositivos cliente usarán para la conexión. De manera predeterminada, se utiliza el puerto 13295.

- En la sección **Alcance**, especifique el alcance al que el punto de distribución distribuirá las actualizaciones (grupos de administración y/o ubicación de red).

- En la sección **Proxy de KSN**, puede configurar la aplicación para que utilice el punto de distribución para reenviar las solicitudes KSN desde los dispositivos administrados.

  - **Habilitar Proxy de KSN en el lado del punto de distribución**

    El servicio de proxy de KSN se ejecuta en el dispositivo que se utiliza como punto de distribución. Utilice esta función para redistribuir y optimizar el tráfico de la red.

    El punto de distribución enviará a Kaspersky las estadísticas de KSN que se enumeran en la declaración de Kaspersky Security Network. De forma predeterminada, la declaración de KSN se encuentra en %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

    Esta opción está deshabilitada de forma predeterminada. Esta opción solo se habilita si las opciones **Usar Servidor de administración como servidor proxy** y **Acepto utilizar Kaspersky Security Network** están habilitadas en la ventana de propiedades del Servidor de administración.

    Puede asignar un nodo de un clúster activo-pasivo a un punto de distribución y habilitar el servidor proxy de KSN en ese nodo.

  - **Reenviar solicitudes KSN al Servidor de administración**

    El punto de distribución envía las solicitudes KSN desde los dispositivos administrados al Servidor de administración.

    Esta opción está activada de forma predeterminada.

  - **Acceder a KSN en la nube/KSN directamente a través de Internet**

    El punto de distribución envía las solicitudes KSN desde los dispositivos administrados a KSN Cloud o a KPSN. Las solicitudes de KSN generadas en el punto de distribución mismo también se envían directamente a la nube de KSN Cloud o a KPSN.

    Los puntos de distribución que tienen instalado el Agente de red versión 11 (o versiones anteriores) no pueden acceder a KPSN directamente. Si desea reconfigurar los puntos de distribución para enviar solicitudes de KSN a KPSN, habilite la opción **Reenviar solicitudes KSN al Servidor de administración** para cada punto de distribución.

    Los puntos de distribución que tienen instalado el Agente de red versión 12 (o una posterior) pueden acceder a KPSN directamente.

  - **No usar el servidor proxy configurado para conectarse a KSN**

    Habilite esta opción, si tiene las configuraciones del servidor proxy configuradas en las propiedades del punto de distribución o en la directiva del Agente de red, pero su arquitectura de red requiere que use KPSN directamente. De lo contrario, las solicitudes de las aplicaciones administradas no podrán llegar a KPSN.

    Esta opción está disponible si selecciona la opción **Acceder a KSN Cloud/KPSN directamente a través de Internet**.

  - **Puerto TCP**

    El número del puerto de TCP que los dispositivos administrados utilizarán para conectarse al Servidor proxy de KSN. El número de puerto predeterminado es 13111.

  - **Puerto UDP**

Si necesita que el Agente de red se conecte al Servidor de administración a través de un puerto UDP, habilite la opción **Usar puerto UDP** y especifique un **número de puerto UDP**. Esta opción está activada de forma predeterminada. El puerto UDP predeterminado para conectarse al Servidor de administración es 15000.

- Puerto HTTPS

  Si necesita que los dispositivos administrados se conecten al servidor proxy de KSN a través de un puerto HTTPS, habilite la opción **Usar HTTPS** y especifique un número de **HTTPS a través del puerto**. El puerto HTTPS predeterminado de conexión al servidor proxy de KSN es 17111.

- En la sección **Descubrimiento de dispositivos**, configure el sondeo de dominios de Windows, Active Directory y rangos de IP por el punto de distribución.

  - Dominios de Windows

    Puede habilitar y programar el descubrimiento de dispositivos en los dominios de Windows.

  - Active Directory

    Puede habilitar y programar el mecanismo de sondeo de red para Active Directory.

    Si utiliza un punto de distribución de Windows, puede seleccionar una de las siguientes opciones:

    - **Sondear el dominio actual de Active Directory**.
    - **Sondear el bosque de dominio de Active Directory**.
    - **Sondear solo los dominios de Active Directory seleccionados**. Si selecciona esta opción, agregue uno o más dominios de Active Directory a la lista.

    Si utiliza un punto de distribución de Linux con la versión 15 del Agente de red instalada, puede sondear solo los dominios de Active Directory para los cuales especifique la dirección y las credenciales de usuario. El sondeo del dominio de Active Directory actual y el bosque de dominios de Active Directory no está disponibles.

  - Intervalos IP

    Puede habilitar el descubrimiento de dispositivos en intervalos IPv4 y en redes IPv6.

    Tras habilitar la opción **Habilitar sondeo de intervalos**, podrá agregar los intervalos que se sondearán y definir una programación para los sondeos. Puede agregar rangos de IP a la lista de rangos analizados.

    Si habilita la opción **Usar Zeroconf para el sondeo de redes IPv6**, el punto de distribución sondeará la red IPv6 automáticamente utilizando Zeroconf, una *tecnología para crear redes sin configuración*. En ese caso, el punto de distribución sondeará la red completa; el sondeo no estará limitado a los intervalos IP que especifique. La opción **Usar Zeroconf para el sondeo de redes IPv6** está disponible si el punto de distribución ejecuta Linux. Para usar el sondeo de Zeroconf IPv6, debe instalar la utilidad avahi-browse en el punto de distribución.

- En la sección **Avanzado**, especifique la carpeta que el punto de distribución debe utilizar para almacenar los datos distribuidos.

- **Usar carpeta predeterminada**

  Si selecciona esta opción, la aplicación utilizará la carpeta de instalación del Agente de red en el punto de distribución.

- **Usar carpeta especificada**

  Si selecciona esta opción, especifique la ruta a la carpeta en el campo que verá debajo. Puede usar una carpeta local del punto de distribución o una carpeta de otro dispositivo conectado a la red corporativa.

  La cuenta de usuario que se utilice para ejecutar el Agente de red en el punto de distribución deberá tener acceso de lectura y escritura a la carpeta especificada.

El dispositivo seleccionado se designa como punto de distribución.

Para que un dispositivo pueda determinar su ubicación de red, debe tener un sistema operativo Windows. No se puede determinar la ubicación de red de dispositivos con otros sistemas operativos.

## Eliminación de un dispositivo de la lista de puntos de distribución

*Para quitar un dispositivo de la lista de puntos de distribución:*

1. En el árbol de consola, haga clic el nodo del **Servidor de administración**.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
3. En la ventana de propiedades del Servidor de administración, en la sección **Puntos de distribución**, seleccione un dispositivo que actúa como punto de distribución y haga clic en el botón **Eliminar**.

El dispositivo desaparece de la lista y deja de actuar como punto de distribución.

No es posible eliminar de la lista de puntos de distribución los dispositivos que el Servidor de administración ha asignado automáticamente.

## Descarga de actualizaciones por puntos de distribución

Kaspersky Security Center permite a los puntos de distribución recibir actualizaciones desde el Servidor de administración, los servidores de Kaspersky o desde una carpeta local o de red.

Si no necesita especificar un origen de actualizaciones, le recomendamos que use la tarea *Descargar actualizaciones a los repositorios de puntos de distribución* para un grupo de administración. Consulte el siguiente tema para obtener más información: Crear la tarea Descargar actualizaciones a los repositorios de puntos de distribución.

*Para configurar la descarga de actualizaciones para un punto de distribución:*

1. En el árbol de consola, haga clic el nodo del **Servidor de administración**.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
3. En la ventana Propiedades del Servidor de administración, en la sección **Puntos de distribución**, seleccione el punto de distribución a través del cual se enviarán las actualizaciones a los dispositivos cliente del grupo.
4. Haga clic en el botón **Propiedades** para abrir la ventana de propiedades del punto de distribución seleccionado.
5. En la ventana de propiedades del punto de distribución, seleccione la sección **Orígenes de actualizaciones**.
6. Seleccione un origen de actualizaciones para el punto de distribución:
   - Para permitir que el punto de distribución reciba actualizaciones del Servidor de administración, seleccione **Recuperar desde el Servidor de administración**:
     - Descargar archivos diff

       Esta opción habilita la función de descarga de archivos diff.

       Esta opción está activada de forma predeterminada.
   - Para permitir que el punto de distribución reciba actualizaciones mediante una tarea, seleccione **Utilizar la tarea para la descarga forzada de actualizaciones**:
     - Haga clic en el botón **Examinar** si tal tarea ya existe en el dispositivo, y seleccione la tarea en la lista respectiva.
     - Haga clic en el botón **Nueva tarea** para crear una tarea si todavía no existe dicha tarea en el dispositivo. Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente.

     La tarea Descargar actualizaciones a los repositorios de puntos de distribución es una tarea local. Debe crear una nueva tarea para cada dispositivo que actúe como punto de distribución.

El punto de distribución recibirá actualizaciones del origen especificado.

# Eliminación de actualizaciones de software desde el repositorio

*Para eliminar actualizaciones de software del repositorio del Servidor de administración:*

1. En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de la consola, seleccione la subcarpeta **Actualizaciones de software**.
2. En el espacio de trabajo de la carpeta **Actualizaciones de software**, seleccione la actualización que desea eliminar.
3. En el menú contextual de la actualización, seleccione **Eliminar archivos de actualización**.

Las actualizaciones de software se eliminarán del repositorio del Servidor de administración.

# Instalación de parches para una aplicación de Kaspersky en modo de clúster

Kaspersky Security Center solo admite la instalación manual de parches para aplicaciones de Kaspersky en el modo de clúster.

*Para instalar un parche para una aplicación de Kaspersky:*

1. Descargue el parche en cada nodo del clúster.
2. Ejecute la instalación del parche en el nodo activo.
3. Espere a que el parche se instale correctamente.
4. Ejecute el parche en todos los subnodos del clúster consecutivamente.

   Si está ejecutando el parche desde la línea de comandos, use la clave `-CLUSTER_SECONDARY_NODE`.

   El parche se instala ahora en todos los nodos del clúster.
5. Ejecute los servicios del clúster de Kaspersky manualmente.

Cada nodo del clúster se muestra en la Consola de administración como un dispositivo con el Agente de red instalado.

Para obtener información sobre los parches instalados, consulte la carpeta **Actualizaciones de software** o el informe sobre las versiones de actualizaciones para módulos de software de aplicaciones de Kaspersky.

# Administración de aplicaciones de terceros en dispositivos cliente

Kaspersky Security Center permite la administración de aplicaciones desarrolladas por Kaspersky y otros proveedores e instaladas en dispositivos cliente.

El administrador puede realizar las siguientes acciones:

- Crear categorías de aplicaciones basadas en criterios específicos.
- Administrar las categorías de aplicaciones utilizando reglas creadas especialmente.
- Administrar aplicaciones que se ejecutan en dispositivos.
- Realizar inventarios y mantener un registro del software instalado en dispositivos cliente.
- Reparar vulnerabilidades en software instalado en dispositivos.
- Instalar actualizaciones desde Windows Update y otros fabricantes de software en dispositivos.
- Supervisar el uso de claves de licencia para grupos de aplicaciones con licencia.

# Acerca de las aplicaciones de terceros

Kaspersky Security Center puede ayudarlo a actualizar y corregir las vulnerabilidades del software de terceros, instalado en los dispositivos cliente. Kaspersky Security Center puede actualizar software de terceros de la versión actual a la última versión únicamente.

La lista de software de terceros puede cambiar y se actualiza dinámicamente. Puede comprobar si puede actualizar el software de terceros (instalado en los dispositivos de los usuarios) con Kaspersky Security Center consultando la lista de actualizaciones disponibles en Kaspersky Security Center Web Console.

El procedimiento que se describe a continuación está destinado únicamente a ver la lista de software de terceros que se puede actualizar con Kaspersky Security Center. Se siguen los pasos para acceder a la información relevante sin iniciar ninguna tarea.

*Para ver la lista del software de terceros que puede actualizar con Kaspersky Security Center en Kaspersky Security Center Web Console:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
3. En el paso **Configuración de tarea nueva** del asistente, especifique estos ajustes:
   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Security Center**.
   b. En el campo **Tipo de tarea**, seleccione **Instalar actualizaciones requeridas y reparar vulnerabilidades**.
4. En el paso **Alcance de la tarea** del asistente, seleccione la opción **Dispositivos administrados**.
5. En el paso del asistente **Elija las reglas de instalación de actualizaciones**, haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Siguiente**.
6. En el paso del asistente **Seleccionar tipo de regla**, seleccione **Regla para actualizaciones de terceros**.
7. En el paso del asistente **Criterios generales**, seleccione la opción **Instalar todas las actualizaciones (excepto las rechazadas)** y, luego, haga clic en **Siguiente**.

Se muestra la lista de software de terceros.

Para ver la lista de software de terceros que puede realizar la actualización con Kaspersky Security Center en una consola basada en MMC, necesita la Licencia de administración de vulnerabilidades y parches. De lo contrario, la tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades** no está disponible.

1. En el árbol de consola, seleccione la carpeta **Dispositivos administrados**.
2. En el espacio de trabajo, seleccione la pestaña **Tareas**.
3. Haga clic en el botón **Crear una tarea** para ejecutar el Asistente para crear nueva tarea. Siga los pasos del asistente.

4. En la página **Seleccione el tipo de tarea**, seleccione **Instalar actualizaciones requeridas y reparar vulnerabilidades**.

5. En el paso del asistente **Elija las reglas de instalación de actualizaciones**, haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Siguiente**.

6. En el paso del asistente **Seleccionar tipo de regla**, seleccione **Regla para actualizaciones de terceros**.

7. En el paso del asistente **Criterios generales**, seleccione la opción **Instalar todas las actualizaciones (excepto las rechazadas)** y, luego, haga clic en **Siguiente**.

Se muestra la lista de software de terceros.

# Instalación de actualizaciones para software de terceros

Kaspersky Security Center permite administrar actualizaciones de software instaladas en dispositivos cliente y reparar vulnerabilidades en aplicaciones de Microsoft y productos de otros fabricantes de software mediante la instalación de actualizaciones requeridas.

Kaspersky Security Center busca actualizaciones a través de la tarea de búsqueda de actualizaciones y las descarga en el repositorio de actualizaciones. Luego de completar la búsqueda de actualizaciones, la aplicación le proporciona al administrador información de las actualizaciones disponibles y las vulnerabilidades en aplicaciones que pueden repararse usando esas actualizaciones.

El servicio de Windows Update proporciona información de las actualizaciones disponibles para Microsoft Windows. Se puede usar el Servidor de administración como el servidor de Windows Server Update Services (WSUS). Para usar el Servidor de administración como servidor de WSUS, debe configurar la sincronización de actualizaciones con Windows Update. Una vez que haya configurado la sincronización de datos con Windows Update, el Servidor de administración proporciona actualizaciones para los servicios de Windows Update en dispositivos, en modo centralizado y con la frecuencia definida.

También puede administrar las actualizaciones de software mediante una directiva del Agente de red. Para hacerlo, debe crear una directiva del Agente de red y configurar actualizaciones de software en la ventana correspondiente del Asistente de nueva directiva.

El administrador puede visualizar una lista de actualizaciones disponibles en la subcarpeta **Actualizaciones de software**, incluida en la carpeta **Administración de aplicaciones**. Esta carpeta contiene una lista de actualizaciones para aplicaciones de Microsoft y productos de otros fabricantes de software, obtenida por el Servidor de administración y que puede ser distribuida a dispositivos. Luego de ver la información de las actualizaciones disponibles, el administrador puede instalarlas en dispositivos.

Para actualizar algunas aplicaciones, Kaspersky Security Center elimina la versión anterior de la aplicación e instala la versión nueva.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedirle al usuario que la cierre.

Asegúrese de que la opción **Mostrar Administración de vulnerabilidades y parches** esté activada en la ventana **Configuración de interfaz** para los servidores de administración principal y secundario. De lo contrario, la tarea de búsqueda de actualizaciones solo se encargará de las actualizaciones de WSUS.

Por seguridad, cada actualización de software de terceros que se instala con la función Administración de vulnerabilidades y parches se somete a un análisis antimalware automático con las tecnologías de Kaspersky Estas tecnologías revisan automáticamente los archivos utilizando técnicas de análisis antivirus, análisis estático, análisis dinámico, análisis de comportamiento en un entorno de pruebas y aprendizaje automático, entre otras.

Los expertos de Kaspersky no realizan análisis manuales de las actualizaciones de software de terceros que puedan instalarse mediante la función Administración de vulnerabilidades y parches. Tampoco buscan vulnerabilidades (conocidas o desconocidas) o funciones no documentadas en las actualizaciones ni las analizan de modos que no se hayan indicado en el párrafo anterior.

Antes de instalar las actualizaciones en todos los dispositivos, puede realizar una instalación de prueba para asegurarse de que las actualizaciones instaladas no causarán fallas en el funcionamiento de las aplicaciones en los dispositivos.

## Procedimiento: Actualización de software de terceros

En esta sección, se describe un escenario para actualizar el software de terceros instalado en los dispositivos cliente. El término “software de terceros” comprende aplicaciones desarrolladas por Microsoft y por otros proveedores de software. Las actualizaciones para las aplicaciones de Microsoft se obtienen a través del servicio Windows Update.

### Requisitos previos

El Servidor de administración debe tener conexión a Internet para instalar actualizaciones de software de terceros que no sean software de Microsoft.

De forma predeterminada, el Servidor de administración no requiere conexión a Internet para instalar las actualizaciones de software de Microsoft en los dispositivos administrados. Los dispositivos administrados pueden descargar las actualizaciones de software de Microsoft directamente de los servidores de Microsoft Update, por ejemplo, o de un servidor Windows Server que esté desplegado en la red de la organización y que tenga Windows Server Update Services (WSUS) habilitado. El Servidor de administración debe estar conectado a Internet cuando utilice el Servidor de administración como servidor WSUS.

## Etapas

El proceso para actualizar aplicaciones de terceros se divide en etapas:

1. **Buscar las actualizaciones requeridas**

   Para buscar las actualizaciones que se requieren para el software de terceros de los dispositivos administrados, ejecute la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Cuando se completa esta tarea, Kaspersky Security Center recibe las listas de vulnerabilidades detectadas y las actualizaciones necesarias para el software de terceros instalado en los dispositivos que especificó en las propiedades de la tarea.

   La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea automáticamente al utilizar el asistente de inicio rápido del Servidor de administración. Si no ejecutó el asistente de inicio rápido, hágalo ahora o cree la tarea.

   Instrucciones:

   - Consola de administración: Análisis de aplicaciones en busca de vulnerabilidades, Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas
   - Kaspersky Security Center Web Console: Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas, Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

2. **Analizar la lista de actualizaciones encontradas**

   Abra la lista **Actualizaciones de software** y decida qué actualizaciones se instalarán. Para obtener información detallada sobre una actualización, haga clic en el nombre de la misma en la lista. Para cada actualización de la lista, también puede ver las estadísticas sobre su instalación en los dispositivos cliente.

   Instrucciones:

   - Consola de administración: Ver información sobre las actualizaciones disponibles
   - Kaspersky Security Center Web Console: Ver información sobre las actualizaciones disponibles para el software de terceros

3. **Configurar la instalación de las actualizaciones**

   Una vez que Kaspersky Security Center cuente con la lista de actualizaciones para el software de terceros, utilice una de dos tareas para instalar las actualizaciones en los dispositivos cliente: la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Instalar actualizaciones de Windows Update*. Cree una de estas tareas. Puede crearlas desde la pestaña **Tareas** o a través de la lista **Actualizaciones de software**.

   La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se utiliza para instalar actualizaciones para aplicaciones de Microsoft (incluidas las actualizaciones que proporciona el servicio Windows Update) y actualizaciones para software de otros proveedores. Tenga en cuenta que esta tarea se puede crear únicamente si se cuenta con una licencia para la función Administración de vulnerabilidades y parches.

   La tarea *Instalar actualizaciones de Windows Update* no requiere licencia, pero solo se la puede utilizar para instalar actualizaciones de Windows Update.

   Para instalar algunas actualizaciones de software, deberá aceptar el Contrato de licencia de usuario final (EULA) para el software de instalación. Si rechaza el EULA, no se instalará la actualización de software correspondiente.

   Puede iniciar una tarea de instalación de actualizaciones según una programación. Si elige configurar una programación, asegúrese de que la tarea de instalación de actualizaciones se ejecute luego de que finalice la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

   Instrucciones:

   - Consola de administración: Reparación de vulnerabilidades en las aplicaciones, Ver información sobre las actualizaciones disponibles

- Kaspersky Security Center Web Console: Creación de la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades, Creación de la tarea Instalar actualizaciones de Windows Update, Ver información sobre las actualizaciones disponibles para el software de terceros

4. **Programar las tareas**

   Para asegurarse de que la lista de actualizaciones siempre esté actualizada, defina una programación que haga que la tarea *Buscar vulnerabilidades y actualizaciones requeridas* se ejecute automáticamente de tanto en tanto. De manera predeterminada, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* está configurada para iniciarse de forma manual.

   Si ha creado la tarea *Instalar actualizaciones necesarias y reparar vulnerabilidades*, puede programarla para que se ejecute con igual o menor frecuencia que la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Al programar la tarea *Instalar actualizaciones de Windows Update*, tenga en cuenta que deberá definir la lista de actualizaciones cada vez que la tarea vaya a iniciarse.

   Cuando programe las tareas, asegúrese de que la tarea de instalación de actualizaciones se inicie después de que la tarea *Buscar vulnerabilidades y actualizaciones requeridas* haya finalizado.

5. **Aprobar y rechazar actualizaciones de software (opcional)**

   Si creó la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades, puede especificar reglas para la instalación de actualizaciones en las propiedades de la tarea. Si creó la tarea Instalar actualizaciones de Windows Update, omita este paso.

   Para cada regla, puede definir las actualizaciones que se instalarán según el estado de la actualización (*Sin definir*, *Aprobada* o *Rechazada*). Si crea una tarea específica para sus servidores, por ejemplo, podría definir una regla que únicamente permita la instalación de actualizaciones que provengan de Windows Update y que tengan el estado *Aprobada*. Tras ello, podría asignar manualmente el estado *Aprobada* a las actualizaciones que desee instalar. Las actualizaciones de Windows Update que tengan el estado *Sin definir* o el estado *Rechazada* no se instalarán en los servidores especificados en la tarea.

   Puede usar el estado *Aprobada* para administrar la instalación de un número modesto de actualizaciones. Cuando necesite instalar muchas actualizaciones, utilice, en cambio, las reglas que puede configurar en la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Asigne el estado *Aprobada* únicamente a las actualizaciones que no cumplan con los criterios indicados en las reglas. Aprobar un gran número de actualizaciones en forma manual afecta el rendimiento del Servidor de administración y puede, incluso, hacer que se sobrecargue.

   De forma predeterminada, las actualizaciones de software descargadas tienen el estado *Sin definir*. Puede cambiar el estado a *Aprobada* o *Rechazada* en la lista **Actualizaciones de software** (**Operaciones** → **Administración de parches** → **Actualizaciones de software**).

   Instrucciones:

   - Consola de administración: Aprobar y rechazar actualizaciones de software
   - Kaspersky Security Center Web Console: Aprobar y rechazar actualizaciones de software de terceros

6. **Configurar el Servidor de administración para que funcione como servidor de Windows Server Update Services (WSUS) (opcional)**

   De manera predeterminada, las actualizaciones de Windows Update se descargan en los dispositivos administrados desde los servidores de Microsoft. Puede cambiar esta configuración para utilizar el Servidor de administración como servidor de WSUS. En este caso, el Servidor de administración sincroniza los datos de la actualización con Windows Update en la frecuencia especificada y proporciona actualizaciones en modo centralizado a Windows Update en los dispositivos en red.

   Para utilizar el Servidor de administración como servidor WSUS, cree la tarea "Sincronización con Windows Update" y marque la casilla **Usar el Servidor de administración como servidor WSUS** en la directiva del Agente de red.

   Instrucciones:

- Consola de administración: Sincronización de las actualizaciones de Windows Update con el Servidor de administración, Configuración de actualizaciones de Windows en una directiva del Agente de red
- Kaspersky Security Center Web Console: Creación de la tarea de sincronización con Windows Update

7. **Ejecutar una tarea de instalación de actualizaciones**

   Inicie la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Instalar actualizaciones de Windows Update*. Al hacerlo, se descargarán las actualizaciones y se las instalará en los dispositivos administrados. Cuando se complete la tarea ejecutada, verifique que su estado en la lista de tareas sea *Completada correctamente*.

8. **Crear el informe sobre los resultados de la instalación de actualizaciones de software de terceros (opcional)**

   Para ver estadísticas detalladas sobre la instalación de las actualizaciones, genere el **Informe sobre los resultados de la instalación de actualizaciones de software de terceros**.

   Instrucciones:

   - Consola de administración: Crear y ver un informe
   - Kaspersky Security Center Web Console: Generar y ver un informe

### Resultados

Si creó y configuró la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, las actualizaciones se instalarán automáticamente en los dispositivos administrados. Cuando se descargan nuevas actualizaciones en el repositorio del Servidor de administración, Kaspersky Security Center verifica si cumplen con los criterios especificados en las reglas de actualización. Todas las actualizaciones nuevas que cumplan con los criterios se instalarán automáticamente la próxima vez que se ejecute la tarea.

Si creó la tarea *Instalar actualizaciones de Windows Update*, solo se instalarán las actualizaciones especificadas en las propiedades de la tarea *Instalar actualizaciones de Windows Update*. En el futuro, si desea instalar nuevas actualizaciones descargadas en el repositorio del Servidor de administración, deberá agregar las actualizaciones necesarias a la lista de actualizaciones de la tarea existente o deberá crear una nueva tarea *Instalar actualizaciones de Windows Update*.

## Visualización de información sobre actualizaciones disponibles para aplicaciones de terceros

*Para ver una lista de las actualizaciones disponibles para las aplicaciones de terceros instaladas en los dispositivos cliente,*

En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de la consola, seleccione la subcarpeta **Actualizaciones de software**.

En el espacio de trabajo de la carpeta, puede visualizar una lista de las actualizaciones disponibles para las aplicaciones instaladas dispositivos.

*Para ver las propiedades de una actualización,*

En el espacio de trabajo de la carpeta **Actualizaciones de software**, en el menú contextual de la actualización, seleccione **Propiedades**.

La siguiente información se encuentra disponible en la ventana Propiedades de la actualización:

- En la sección **General**, puede ver el **Estado de aprobación de la actualización**:
  - **No definida**: la actualización está disponible en la lista de actualizaciones, pero no se ha autorizado su instalación.
  - **Aprobada**: la actualización está disponible en la lista de actualizaciones y se ha autorizado su instalación.
  - **Rechazada**: se ha prohibido la instalación de la actualización.
- En la sección **Atributos**, puede ver los valores del campo **Instalado automáticamente**:
  - El valor **Automáticamente** se muestra si la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* puede instalar actualizaciones de la aplicación. La tarea instala automáticamente las nuevas actualizaciones de la dirección web proporcionada por el proveedor de software de terceros.
  - El valor **Manual** se muestra si Kaspersky Security Center no puede instalar las actualizaciones de la aplicación de modo automático. Puede instalar las actualizaciones de manera manual.

  El campo **Instalado automáticamente** no se muestra para las actualizaciones de la aplicación de Windows.
- Lista de dispositivos cliente para los cuales se destina la actualización.
- Lista de componentes del sistema (requisitos previos) que se deben instalar antes de la actualización (si existe).
- Vulnerabilidades de software que solucionará la actualización.

## Aprobar y rechazar actualizaciones de software

Una tarea de instalación de actualizaciones puede estar configurada para requerir la aprobación de las actualizaciones que se deban instalar. Puede aprobar las actualizaciones que deban instalarse y rechazar las que no deban instalarse.

Podría suceder, por ejemplo, que quiera instalar las actualizaciones en un entorno de prueba para verificar primero que no interfieran con el funcionamiento de los dispositivos, y solo entonces, en caso de no haber problemas, permitir que se instalen en los dispositivos cliente.

Puede usar el estado *Aprobada* para administrar la instalación de un número modesto de actualizaciones de terceros. Cuando necesite instalar muchas actualizaciones de terceros, utilice, en cambio, las reglas que puede configurar en la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Asigne el estado *Aprobada* únicamente a las actualizaciones que no cumplan con los criterios indicados en las reglas. Aprobar un gran número de actualizaciones en forma manual afecta el rendimiento del Servidor de administración y puede, incluso, hacer que se sobrecargue.

*Para aprobar o rechazar una o más actualizaciones:*

1. En el árbol de consola, seleccione el nodo **Avanzado → Administración de aplicaciones → Actualizaciones de software**.
2. En el espacio de trabajo de la carpeta **Actualizaciones de software**, haga clic en el botón **Actualizar** en la esquina superior derecha. Aparece una lista de actualizaciones.

3. Seleccione las actualizaciones que desee aprobar o rechazar.

   El cuadro de información para los objetos seleccionados aparece en el lado derecho del espacio de trabajo.

4. En la lista desplegable **Estado de aprobación de la actualización**, seleccione **Aprobada** para aprobar las actualizaciones seleccionadas o **Rechazada** para rechazar las actualizaciones seleccionadas.

   El valor predeterminado es **No definida**.

Las actualizaciones para las que establece el estado **Aprobada** se colocan en una cola para la instalación.

Las actualizaciones para las cuales configure el estado **Rechazada** se desinstalarán (si es posible) de todos los dispositivos en los cuales se instalaron anteriormente. Estas actualizaciones no se instalarán en otros dispositivos en el futuro.

Existen actualizaciones para las aplicaciones de Kaspersky que no se pueden desinstalar. Si configura el estado **Rechazada** para ellas, Kaspersky Security Center no desinstalará estas actualizaciones de los dispositivos en los cuales se hayan instalado anteriormente. Sin embargo, se abstendrá de instalarlas en otros dispositivos en el futuro. Si no se puede desinstalar una actualización para las aplicaciones de Kaspersky, esta propiedad se muestra en la ventana de propiedades de actualización: en el panel **Secciones**, seleccione **General**, y en el espacio de trabajo, la propiedad aparecerá en **Requisitos de instalación**. Si configura el estado **Rechazada** para las actualizaciones de software de terceros, estas actualizaciones no se instalarán en los dispositivos cuya instalación se haya planeado pero aún no se haya realizado. Las actualizaciones permanecerán en los dispositivos en los cuales ya se hayan instalado. Si necesita eliminar estas actualizaciones, hágalo manualmente en forma local.

## Sincronización de las actualizaciones de Windows Update con el Servidor de administración

Si seleccionó **Usar el Servidor de administración como servidor WSUS** en la ventana **Opciones de administración de actualizaciones** del Asistente de inicio rápido, la tarea de sincronización con Windows Update se crea automáticamente. Puede ejecutar la tarea en la carpeta **Tareas**. La funcionalidad de una actualización de software de Microsoft solo se encuentra disponible luego de que la tarea **Sincronización con Windows Update** se complete correctamente.

Las actualizaciones de software de Microsoft pueden superar los 10 GB. Asegúrese de que la base de datos del Servidor de administración sea capaz de albergar dichos volúmenes; de lo contrario, la tarea **Sincronización con Windows Update** fallará. La base de datos de Microsoft SQL Express no es compatible con la tarea **Sincronización con Windows Update**.

La tarea **Sincronización con Windows Update** solo descarga metadatos de los servidores de Microsoft. Si la red no emplea ningún servidor de WSUS, cada dispositivo cliente descarga por su propia cuenta las actualizaciones de Microsoft desde servidores externos.

*Para crear una tarea para la sincronización de las actualizaciones de Windows con el Servidor de administración, haga lo siguiente:*

1. En la carpeta **Avanzado → Administración de aplicaciones** del árbol de la consola, seleccione la subcarpeta **Actualizaciones de software**.

2. Haga clic en el botón **Acciones adicionales** y seleccione **Configurar la sincronización con Windows Update** en la lista desplegable.

   El Asistente crea la tarea **Sincronización con Windows Update** que se muestra en la carpeta **Tareas**.

   Inicia el Asistente de creación de la tarea de recuperación de datos del centro de actualizaciones de Windows. Siga las instrucciones del asistente.

También puede crear la tarea de sincronización con Windows Update en la carpeta **Tareas** haciendo clic en **Crear una tarea**.

Microsoft elimina con regularidad actualizaciones desactualizadas de los servidores de la empresa para que el número de actualizaciones vigentes siempre sea entre 200 000 y 300 000. Para reducir el uso del espacio en disco y el tamaño de la base de datos, Kaspersky Security Center elimina las actualizaciones obsoletas que ya no están presentes en los servidores de actualización de Microsoft.

Al ejecutar la tarea **Sincronización con Windows Update**, la aplicación recibe una lista de actualizaciones vigentes de un servidor de actualizaciones de Microsoft. Luego, Kaspersky Security Center compila una lista de actualizaciones que se han desactualizado. Al siguiente inicio de la tarea **Buscar vulnerabilidades y actualizaciones requeridas**, Kaspersky Security Center marca todas las actualizaciones desactualizadas y configura su momento de eliminación. Al siguiente inicio de la tarea **Sincronización con Windows Update**, se eliminan todas las actualizaciones marcadas para su eliminación hace 30 días. Kaspersky Security Center también comprueba las actualizaciones desactualizadas que se marcaron para su eliminación hace más de 180 días y, luego, elimina estas actualizaciones más antiguas.

Cuando se completa la tarea **Sincronización con Windows Update** y se eliminan las actualizaciones desactualizadas, es posible que la base de datos aún tenga los códigos hash pertenecientes a los archivos de las actualizaciones eliminadas, así como los archivos correspondientes en los archivos de %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles (si se descargaron anteriormente). Puede ejecutar la tarea **Mantenimiento del Servidor de administración** para eliminar estos registros desactualizados de la base de datos y de los archivos correspondientes.

## Paso 1. Definir la reducción de tráfico

Cuando Kaspersky Security Center realiza la sincronización de actualizaciones con los servidores de Windows Update, guarda información sobre todos los distintos archivos en la base de datos del Servidor de administración. Todos los archivos requeridos para una actualización también se descargan a la unidad durante la interacción con el Agente de Windows Update. En particular, Kaspersky Security Center guarda la información sobre archivos de actualización expresos en la base de datos y los descarga cuando sea necesario. Descargar archivos de actualización rápida genera una reducción del espacio libre en la unidad.

Para evitar una disminución en el volumen del espacio de disco y reducir el tráfico, deshabilite la casilla **Descargar archivos de instalación rápida**.

Si se selecciona esta opción, los archivos de actualización expresos se descargan al ejecutar la tarea. Esta opción no está seleccionada de manera predeterminada.

## Paso 2. Aplicaciones

En esta sección puede seleccionar las aplicaciones para las cuales se descargarán las actualizaciones.

Si la casilla **Todas las aplicaciones** se selecciona, las actualizaciones se descargarán para todas las aplicaciones existentes, y para todas las aplicaciones que se puedan publicar en el futuro.

De forma predeterminada, la casilla **Todas las aplicaciones** está marcada.

## Paso 3. Categorías de actualizaciones

En esta sección, puede seleccionar las categorías de las actualizaciones que se descargarán en el Servidor de administración.

Si la casilla **Todas las categorías** se selecciona, las actualizaciones se descargarán para todas las categorías de actualizaciones existentes, y para todas las categorías que se puedan publicar en el futuro.

De forma predeterminada, la casilla **Todas las categorías** está marcada.

## Paso 4. Idiomas de actualizaciones

En esta ventana, puede seleccionar los idiomas de localización de las actualizaciones que se descargarán en el Servidor de administración. Seleccione una de las opciones siguientes para descargar idiomas de localización de actualizaciones:

- **Descargar todos los idiomas, incluidos los nuevos**

  Si se selecciona esta opción, todos los idiomas de localización de las actualizaciones disponibles se descargarán en el Servidor de administración. Esta opción está seleccionada de forma predeterminada.

- **Descargar los idiomas seleccionados**

  Si se selecciona esta opción, podrá elegir de la lista los idiomas de localización de las actualizaciones que se descargarán en el Servidor de administración.

## Paso 5. Selección de una cuenta para iniciar la tarea

En la ventana **Seleccione una cuenta para ejecutar la tarea**, puede especificar que cuenta usar al ejecutar la tarea. Seleccione una de las siguientes opciones:

- **Cuenta predeterminada**

  La tarea se ejecutará utilizando la misma cuenta que la aplicación que realizará la tarea.

  Esta opción está seleccionada de forma predeterminada.

- **Especificar cuenta**

  Complete los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta con la que se ejecutará la tarea. La cuenta debe tener los derechos necesarios para realizar la tarea.

  - **Cuenta**

    Cuenta con la que se ejecutará la tarea.

  - **Contraseña**

    Contraseña de la cuenta con la que se ejecutará la tarea.

## Paso 6. Configuración de una programación de inicio para la tarea

En la página **Configurar programación de tarea**, puede crear una planificación para el inicio de la tarea. De ser necesario, configure los siguientes ajustes:

- **Inicio programado:**

  Seleccione y configure la programación según la cual se ejecutará la tarea.

  - **Cada N horas**

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

    De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

  - **Cada N días**

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

    De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

  - **Cada N semanas**

    La tarea se ejecutará periódicamente, a intervalos regulares, en el día de la semana y a la hora que especifique. Cada ejecución estará separada de la anterior por el número de semanas que indique.

    Por defecto, la tarea se ejecutará cada lunes a la hora actual del sistema.

  - **Cada N minutos**

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

    De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

  - **Diario (no compatible con horario de verano)**

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta programación no tiene en cuenta los cambios de horario estacionales. La hora de inicio de la tarea se mantendrá sin cambios incluso si el reloj se atrasa o se adelanta una hora debido al horario de verano.

    No recomendamos usar esta programación. Se la ofrece para mantener la compatibilidad con versiones anteriores de Kaspersky Security Center.

    De forma predeterminada, la tarea se iniciará todos los días a la hora actual del sistema.

- **Semanal**

  La tarea se ejecutará cada semana en el día y a la hora que indique.

- **Por días de la semana**

  La tarea se ejecutará periódicamente en los días de la semana y a la hora que indique.

  De manera predeterminada, la tarea se ejecutará todos los viernes a las 18:00:00.

- **Mensual**

  La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

  Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

  Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

- **Manual**

  La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

  Esta opción está seleccionada de forma predeterminada.

- **Una vez**

  La tarea se ejecuta una vez, en la fecha y hora especificadas (de manera predeterminada, el día en que se creó la tarea).

- **Cada mes en los días especificados de semanas seleccionadas**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  por defecto, la hora de inicio es a las 18:00 y no se selecciona ningún día del mes.

  > Tenga en cuenta que no selecciona una fecha específica en el mes, ni el número de la semana (primera, segunda semana del mes), sino el número de secuencia del día de la semana dentro de un mes. Por ejemplo, si coloca el cursor en la celda Tu de la Primera fila, significa que la tarea se ejecutará el primer martes de cada mes nuevo.**MaPrimero**

  Puede seleccionar varios días de la semana.

- **Ante brotes de virus**

La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

- Antivirus para estaciones de trabajo y servidores de archivos
- Antivirus para defensa del perímetro
- Antivirus para sistemas de correo

Por defecto, están seleccionados todos los tipos de aplicaciones.

En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- **Al completarse otra tarea**

  La tarea actual se iniciará después de que se complete otra tarea. Esta opción solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

- **Ejecutar tareas no realizadas**

  Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

  Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

  Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

  Esta opción está deshabilitada de forma predeterminada.

- Esperar un tiempo definido al azar antes de iniciar la tarea

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

- Limitar el tiempo de espera a esta cantidad de minutos

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

  Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

### Paso 7. Definición del nombre de la tarea

En la ventana **Defina el nombre de la tarea**, especifique el nombre para la tarea que está creando. Un nombre de tarea no puede tener más de 100 caracteres y no puede incluir ningún carácter especial ( `"*<>?\:|` ). El valor predeterminado es *Realizar la sincronización con Windows Update*.

### Paso 8. Completar creación de la tarea

En la ventana **Finalizar la creación de la tarea**, haga clic en el botón **Finalizar** para completar el Asistente.

Para que la tarea se inicie en cuanto se cierre el asistente, marque la casilla **Ejecutar la tarea al finalizar el asistente**.

La tarea de sincronización con Windows Update recién creada aparecerá en la lista de tareas en la carpeta **Tareas** del árbol de la consola.

## Instalación de actualizaciones en dispositivos manualmente

Si seleccionó **Buscar e instalar actualizaciones requeridas** en la página **Opciones de administración de actualizaciones** del Asistente de inicio rápido, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se crea automáticamente. Puede iniciar o detener la tarea en la carpeta **Dispositivos administrados** en la pestaña **Tareas**.

Si seleccionó **Buscar actualizaciones requeridas** en el Asistente de inicio rápido, puede instalar las actualizaciones de software en dispositivos cliente mediante la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

Puedes hacer lo siguiente:

- Crear una tarea para instalar actualizaciones.
- Agregue una regla para instalar una actualización en una tarea de instalación de actualización existente.
- En la configuración de una tarea de instalación de actualización existente, configure una instalación de prueba de actualizaciones.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedirle al usuario que la cierre.

## Instalar actualizaciones creando una tarea de instalación

Puedes hacer lo siguiente:

- Crear una tarea para instalar ciertas actualizaciones.
- Seleccionar una actualización y crear una tarea para instalar esa y otras actualizaciones similares.

*Para instalar actualizaciones específicas:*

1. En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de la consola, seleccione la subcarpeta **Actualizaciones de software**.
2. En el espacio de trabajo, seleccione las actualizaciones que desea instalar.
3. Realice cualquiera de las siguientes acciones:
   - Haga clic derecho en una de las actualizaciones seleccionadas de la lista y, a continuación, seleccione **Instalar actualización** → **Nueva tarea**.
   - Haga clic en el vínculo **Instalar actualización (crear tarea)** en el cuadro de información de las actualizaciones seleccionadas.
4. Haga su elección en la ventana que aparece sobre la instalación de todas las actualizaciones de aplicaciones anteriores. Haga clic en **Sí** si está de acuerdo con la instalación de versiones sucesivas de la aplicación de forma incremental si es necesario para instalar las actualizaciones seleccionadas. Haga clic en **No** si desea actualizar las aplicaciones de forma sencilla, sin necesidad de instalar versiones sucesivas. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

   El Asistente de creación de tareas de instalación de actualizaciones y reparación de vulnerabilidades se inicia. Siga los pasos del asistente.

5. En la página **Seleccione la opción de reinicio del sistema operativo** del asistente, seleccione la acción a realizar cuando el sistema operativo de los dispositivos cliente deba reiniciarse después de la operación:

- **No reiniciar el dispositivo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

- **Reiniciar el dispositivo**

  Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

  Esta opción está seleccionada de forma predeterminada.

  - **Repetir solicitud cada (min)**

    Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

    Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

    Si no habilita esta opción, la solicitud se mostrará una sola vez.

  - **Reiniciar después de (min)**

    Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

    Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de aplicaciones en sesiones bloqueadas**

Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

Esta opción está deshabilitada de forma predeterminada.

6. En la página **Configurar programación de tarea** del asistente, puede crear una programación para el inicio de la tarea. De ser necesario, configure los siguientes ajustes:

- Inicio programado:

  Seleccione y configure la programación según la cual se ejecutará la tarea.

  - Cada N horas

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

    De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

  - Cada N días

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

    De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

  - Cada N semanas

    La tarea se ejecutará periódicamente, a intervalos regulares, en el día de la semana y a la hora que especifique. Cada ejecución estará separada de la anterior por el número de semanas que indique.

    Por defecto, la tarea se ejecutará cada lunes a la hora actual del sistema.

  - Cada N minutos

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

    De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

  - Diario (no compatible con horario de verano)

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta programación no tiene en cuenta los cambios de horario estacionales. La hora de inicio de la tarea se mantendrá sin cambios incluso si el reloj se atrasa o se adelanta una hora debido al horario de verano.

    No recomendamos usar esta programación. Se la ofrece para mantener la compatibilidad con versiones anteriores de Kaspersky Security Center.

    De forma predeterminada, la tarea se iniciará todos los días a la hora actual del sistema.

  - Semanal

La tarea se ejecutará cada semana en el día y a la hora que indique.

- **Por días de la semana**

  La tarea se ejecutará periódicamente en los días de la semana y a la hora que indique.

  De manera predeterminada, la tarea se ejecutará todos los viernes a las 18:00:00.

- **Mensual**

  La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

  Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

  Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

- **Manual**

  La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

  Esta opción está seleccionada de forma predeterminada.

- **Cada mes en los días especificados de semanas seleccionadas**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  de forma predeterminada, la hora de inicio es a las 18:00 y no se selecciona ningún día del mes.

  Tenga en cuenta que no selecciona una fecha específica en el mes, ni el número de la semana (primera, segunda semana del mes), sino el número de secuencia del día de la semana dentro de un mes. Por ejemplo, si coloca el cursor en la celda Tu de la Primera fila, significa que la tarea se ejecutará el primer martes de cada mes nuevo.**MaPrimero**

  Puede seleccionar varios días de la semana.

- **Ante brotes de virus**

  La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para defensa del perímetro
  - Antivirus para sistemas de correo

  Por defecto, están seleccionados todos los tipos de aplicaciones.

  En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- **Al completarse otra tarea**

  La tarea actual se iniciará después de que se complete otra tarea. Esta opción solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

- **Ejecutar tareas no realizadas**

  Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

  Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

  Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

  Esta opción está deshabilitada de forma predeterminada.

- **Esperar un tiempo definido al azar antes de iniciar la tarea**

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

- **Limitar el tiempo de espera a esta cantidad de minutos**

Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

7. En la página **Defina el nombre de la tarea** del asistente, especifique el nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).

8. En la página **Finalizar la creación de la tarea** del asistente, haga clic en el botón **Finalizar** para cerrar el asistente.

   Para que la tarea se inicie en cuanto se cierre el asistente, marque la casilla **Ejecutar la tarea al finalizar el asistente**.

Después de que el asistente termina su operación, aparece la opción **Instalar actualizaciones requeridas y reparar vulnerabilidades** en la carpeta **Tareas**.

Puede habilitar la instalación automática de los componentes del sistema (requisitos previos) antes de la instalación de una actualización en las propiedades de la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Cuando esta opción esté habilitada, todos los componentes del sistema requeridos se instalan antes de la actualización. Puede encontrarse una lista de los componentes requeridos en las propiedades de la actualización.

En las propiedades de la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede permitir la instalación de actualizaciones que actualizan la aplicación a una nueva versión.

Si la configuración de la tarea proporciona reglas para la instalación de actualizaciones de terceros, el Servidor de administración descarga todas las actualizaciones relevantes desde los sitios web de sus proveedores. Las actualizaciones se guardan en el repositorio del Servidor de administración y luego se distribuyen e instalan en dispositivos donde son aplicables.

Si la configuración de la tarea proporciona reglas para la instalación de actualizaciones de Microsoft y el Servidor de administración actúa como servidor WSUS, el Servidor de administración descarga todas las actualizaciones relevantes en el repositorio y luego las distribuye a dispositivos administrados. Si la red no emplea ningún servidor de WSUS, cada dispositivo cliente descarga por su propia cuenta las actualizaciones de Microsoft desde servidores externos.

*Para instalar una determinada actualización y otras similares:*

1. En la carpeta **Avanzado → Administración de aplicaciones** del árbol de la consola, seleccione la subcarpeta **Actualizaciones de software**.

2. En el espacio de trabajo, seleccione la actualización que desea instalar.

3. Haga clic en el botón **Ejecutar el Asistente de instalación de actualizaciones**.

   Se iniciará el Asistente de instalación de actualizaciones.

   > Para usar las funciones del Asistente de instalación de actualizaciones, debe tener una licencia de Administración de vulnerabilidades y parches.

   Siga los pasos del asistente.

4. En la página **Buscar tareas de instalación de actualizaciones existentes**, especifique la siguiente configuración:

   - **Buscar tareas que instalen esta actualización**

     Si esta opción está activada, el Asistente de instalación de actualizaciones busca las tareas existentes que instalan la actualización seleccionada.

     Si esta opción está desactivada o si la búsqueda no recupera ninguna tarea aplicable, el Asistente de instalación de actualizaciones le pedirá que cree una regla o tarea para la instalación de la actualización.

     Esta opción está activada de forma predeterminada.

   - **Aprobar la instalación de la actualización**

     Se aprobará la instalación de la actualización seleccionada. Habilite esta opción si ha aplicado reglas de instalación de actualizaciones que solo permitan instalar actualizaciones aprobadas.

     Esta opción está deshabilitada de forma predeterminada.

5. Si decide buscar tareas de instalación de actualizaciones existentes y si la búsqueda recupera algunas tareas, puede ver las propiedades de estas tareas o iniciarlas manualmente. No se requieren más acciones.

   De lo contrario, haga clic en el botón **Nueva tarea de instalación de actualizaciones**.

6. Seleccione el tipo de regla de instalación que desea agregar a la nueva tarea y, a continuación, haga clic en el botón **Finalizar**.

7. Haga su elección en la ventana que aparece sobre la instalación de todas las actualizaciones de aplicaciones anteriores. Haga clic en **Sí** si está de acuerdo con la instalación de versiones sucesivas de la aplicación de forma incremental si es necesario para instalar las actualizaciones seleccionadas. Haga clic en **No** si desea actualizar las aplicaciones de forma sencilla, sin necesidad de instalar versiones sucesivas. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

   El Asistente de creación de tareas de instalación de actualizaciones y reparación de vulnerabilidades se inicia. Siga los pasos del asistente.

8. En la página **Seleccione la opción de reinicio del sistema operativo** del asistente, seleccione la acción a realizar cuando el sistema operativo de los dispositivos cliente deba reiniciarse después de la operación:

- **No reiniciar el dispositivo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

- **Reiniciar el dispositivo**

  Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

  Esta opción está seleccionada de forma predeterminada.

  - **Repetir solicitud cada (min)**

    Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

    Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

    Si no habilita esta opción, la solicitud se mostrará una sola vez.

  - **Reiniciar después de (min)**

    Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

    Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de aplicaciones en sesiones bloqueadas**

Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

Esta opción está deshabilitada de forma predeterminada.

9. En la página **Seleccionar dispositivos a los que se asignará la tarea** del asistente, seleccione una de las siguientes opciones:

- **Seleccionar dispositivos de la red detectados por el Servidor de administración**

  La tarea se asignará a ciertos dispositivos específicos. Estos pueden ser tanto dispositivos asignados a grupos de administración como dispositivos no asignados.

  Podría usar esta opción para, por ejemplo, una tarea que instale el Agente de red en los dispositivos que no estén asignados a un grupo de administración.

- **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**

  Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

  Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.

- **Asignar tarea a una selección de dispositivos**

  La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

  Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

- **Asignar tarea a un grupo de administración**

  La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

  Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

  Si la tarea se asigna a un grupo de administración, la pestaña **Seguridad** no se mostrará en la ventana de propiedades de la tarea; esto se debe a que las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

10. En la página **Configurar programación de tarea** del asistente, puede crear una programación para el inicio de la tarea. De ser necesario, configure los siguientes ajustes:

- Inicio programado:

  Seleccione y configure la programación según la cual se ejecutará la tarea.

  - Cada N horas

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

    De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

  - Cada N días

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

    De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

  - Cada N semanas

    La tarea se ejecutará periódicamente, a intervalos regulares, en el día de la semana y a la hora que especifique. Cada ejecución estará separada de la anterior por el número de semanas que indique.

    Por defecto, la tarea se ejecutará cada lunes a la hora actual del sistema.

  - Cada N minutos

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

    De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

  - Diario (no compatible con horario de verano)

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta programación no tiene en cuenta los cambios de horario estacionales. La hora de inicio de la tarea se mantendrá sin cambios incluso si el reloj se atrasa o se adelanta una hora debido al horario de verano.

    No recomendamos usar esta programación. Se la ofrece para mantener la compatibilidad con versiones anteriores de Kaspersky Security Center.

    De forma predeterminada, la tarea se iniciará todos los días a la hora actual del sistema.

  - Semanal

La tarea se ejecutará cada semana en el día y a la hora que indique.

- **Por días de la semana**

  La tarea se ejecutará periódicamente en los días de la semana y a la hora que indique.

  De manera predeterminada, la tarea se ejecutará todos los viernes a las 18:00:00.

- **Mensual**

  La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

  Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

  Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

- **Manual** (opción seleccionada por defecto)

  La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

  Esta opción está seleccionada de forma predeterminada.

- **Cada mes en los días especificados de semanas seleccionadas**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  Por defecto, la hora de inicio es a las 18:00 y no se selecciona ningún día del mes.

  Tenga en cuenta que no selecciona una fecha específica en el mes, ni el número de la semana (primera, segunda semana del mes), sino el número de secuencia del día de la semana dentro de un mes. Por ejemplo, si coloca el cursor en la celda Tu de la Primera fila, significa que la tarea se ejecutará el primer martes de cada mes nuevo.**MaPrimero**

  Puede seleccionar varios días de la semana.

- **Ante brotes de virus**

  La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para defensa del perímetro
  - Antivirus para sistemas de correo

  Por defecto, están seleccionados todos los tipos de aplicaciones.

  En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- **Al completarse otra tarea**

  La tarea actual se iniciará después de que se complete otra tarea. Esta opción solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

- **Ejecutar tareas no realizadas**

  Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

  Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

  Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

  Esta opción está deshabilitada de forma predeterminada.

- **Limitar el tiempo de espera a esta cantidad de minutos**

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

- **Limitar el tiempo de espera a esta cantidad de minutos**

Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

11. En la página **Defina el nombre de la tarea** del asistente, especifique el nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).

12. En la página **Finalizar la creación de la tarea** del asistente, haga clic en el botón **Finalizar** para cerrar el asistente.

    Para que la tarea se inicie en cuanto se cierre el asistente, marque la casilla **Ejecutar la tarea al finalizar el asistente**.

Cuando el asistente termina, se crea la tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades** y se la muestra en la carpeta **Tareas**.

Además de los ajustes configurados durante el proceso de creación, la tarea tiene otras propiedades que se pueden modificar.

La actualización a una nueva versión de la aplicación puede provocar el mal funcionamiento de las aplicaciones dependientes en dispositivos.

## Instalar una actualización agregando una regla a una tarea de instalación existente

*Para instalar una actualización agregando una regla a una tarea de instalación existente:*

1. En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de la consola, seleccione la subcarpeta **Actualizaciones de software**.

2. En el espacio de trabajo, seleccione la actualización que desea instalar.

3. Haga clic en el botón **Ejecutar el Asistente de instalación de actualizaciones**.

   Se iniciará el Asistente de instalación de actualizaciones.

   Para usar las funciones del Asistente de instalación de actualizaciones, debe tener una licencia de Administración de vulnerabilidades y parches.

   Siga los pasos del asistente.

4. En la página **Buscar tareas de instalación de actualizaciones existentes**, especifique la siguiente configuración:

   - **Buscar tareas que instalen esta actualización**

     Si esta opción está activada, el Asistente de instalación de actualizaciones busca las tareas existentes que instalan la actualización seleccionada.

     Si esta opción está desactivada o si la búsqueda no recupera ninguna tarea aplicable, el Asistente de instalación de actualizaciones le pedirá que cree una regla o tarea para la instalación de la actualización.

     Esta opción está activada de forma predeterminada.

   - **Aprobar la instalación de la actualización**

     Se aprobará la instalación de la actualización seleccionada. Habilite esta opción si ha aplicado reglas de instalación de actualizaciones que solo permitan instalar actualizaciones aprobadas.

     Esta opción está deshabilitada de forma predeterminada.

5. Si decide buscar tareas de instalación de actualizaciones existentes y si la búsqueda recupera algunas tareas, puede ver las propiedades de estas tareas o iniciarlas manualmente. No se requieren más acciones.

   De lo contrario, haga clic en el botón **Agregar regla de instalación de actualizaciones**.

6. Seleccione la tarea a la que desea agregar una regla y luego haga clic en el botón **Agregar regla**.

   Además, puede ver las propiedades de las tareas existentes, iniciarlas manualmente o crear una nueva tarea.

7. Seleccione el tipo de regla que se agregará a la tarea seleccionada y luego haga clic en el botón **Finalizar**.

8. Haga su elección en la ventana que aparece sobre la instalación de todas las actualizaciones de aplicaciones anteriores. Haga clic en **Sí** si está de acuerdo con la instalación de versiones sucesivas de la aplicación de forma incremental si es necesario para instalar las actualizaciones seleccionadas. Haga clic en **No** si desea actualizar las aplicaciones de forma sencilla, sin necesidad de instalar versiones sucesivas. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

Se agrega una nueva regla para instalar la actualización a la tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades**.

## Configurar una instalación de prueba de las actualizaciones

*Para configurar una instalación de prueba de las actualizaciones:*

1. En el árbol de consola, seleccione la tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades** en la carpeta **Dispositivos administrados**, en la pestaña **Tareas**.

2. En el menú contextual de la tarea, seleccione **Propiedades**.

   Se abre la ventana de propiedades de la tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades**.

3. En la ventana de propiedades de la tarea, en la sección **Instalación de prueba**, seleccione una de las opciones disponibles para la instalación de prueba:

   - **No analizar**. Seleccione esta opción si no desea realizar una instalación de prueba de las actualizaciones.
   - **Ejecutar análisis en los dispositivos seleccionados**. Seleccione esta opción si desea probar la instalación de actualizaciones en dispositivos seleccionados. Haga clic en el botón **Agregar** y seleccione los dispositivos en los que necesita realizar una instalación de prueba de las actualizaciones.
   - **Ejecutar análisis en los dispositivos del grupo especificado**. Seleccione esta opción si desea probar la instalación de actualizaciones en un grupo de dispositivos. En el campo **Especifique un grupo de prueba**, indique un grupo de dispositivos en el que desee realizar una instalación de prueba.
   - **Ejecutar análisis en el porcentaje de dispositivos especificado**. Seleccione esta opción si desea probar la instalación de actualizaciones en una parte de los dispositivos. En el campo **Porcentaje de dispositivos de prueba en relación con todos los dispositivos de destino**, especifique el porcentaje de dispositivos en el que desea realizar una instalación de prueba de las actualizaciones.

4. Una vez que haya seleccionado cualquier opción excepto **No analizar**, en el campo **Cantidad de tiempo para tomar la decisión de si se debe continuar la instalación, en horas**, especifique el número de horas que deben transcurrir desde la instalación de prueba de las actualizaciones hasta el inicio de la instalación de las actualizaciones en todos los dispositivos.

## Configuración de actualizaciones de Windows en una directiva del Agente de red

*Para configurar las actualizaciones de Windows en una directiva del Agente de red:*

1. En el árbol de la consola, seleccione **Dispositivos administrados**.
2. En el espacio de trabajo, seleccione la pestaña **Directivas**.
3. Seleccione una directiva de Agente de red.
4. En el menú contextual de la directiva, seleccione **Propiedades**.

   Se abre la ventana de propiedades correspondiente a la directiva del Agente de red.

5. En el panel **Secciones**, seleccione **Actualizaciones y vulnerabilidades de software**.
6. Seleccione la opción **Usar el Servidor de administración como servidor WSUS** si desea que las actualizaciones de Windows se descarguen al Servidor de administración y luego se distribuyan a los dispositivos cliente por medio del Agente de red.

   Si no se selecciona esta opción, las actualizaciones de Windows se descargarán al Servidor de administración. En tal caso, los dispositivos cliente reciben las actualizaciones directamente desde los servidores de Windows.

7. Seleccione el conjunto de actualizaciones que los usuarios pueden instalar manualmente en sus dispositivos mediante Windows Update.

Si selecciona una nueva opción en **Permitir que los usuarios administren la instalación de actualizaciones de Windows Update** luego de que Windows Update encuentre actualizaciones para un dispositivo con Windows 10, la nueva opción no entrará en vigor sino hasta que se instalen esas actualizaciones.

Seleccione un elemento en la lista desplegable:

- **Permitir a los usuarios instalar todas las actualizaciones de Windows Update aplicables**

  Los usuarios podrán instalar cualquier actualización de Microsoft Windows Update que resulte adecuada para sus dispositivos.

  Seleccione esta opción si prefiere no interferir en la instalación de actualizaciones.

  Cuando un usuario instala actualizaciones de Microsoft Windows Update manualmente, puede suceder que los archivos de actualización se descarguen de los servidores de Microsoft y no del Servidor de administración. Esto puede ocurrir si el Servidor de administración no ha descargado aún esas actualizaciones. Descargar actualizaciones de los servidores de Microsoft genera tráfico adicional.

- **Permitir a los usuarios instalar solo actualizaciones aprobadas de Windows Update**

  Los usuarios podrán instalar cualquier actualización de Microsoft Windows Update que resulte adecuada para sus dispositivos y que usted haya aprobado.

  Podría suceder, por ejemplo, que primero quiera instalar las actualizaciones en un entorno de prueba para verificar que no interfieran con el funcionamiento de los dispositivos, y solo entonces, en caso de no detectarse problemas, permitir que las actualizaciones aprobadas se instalen en los dispositivos cliente.

  Cuando un usuario instala actualizaciones de Microsoft Windows Update manualmente, puede suceder que los archivos de actualización se descarguen de los servidores de Microsoft y no del Servidor de administración. Esto puede ocurrir si el Servidor de administración no ha descargado aún esas actualizaciones. Descargar actualizaciones de los servidores de Microsoft genera tráfico adicional.

- **No permitir que los usuarios instalen actualizaciones de Windows Update**

  Los usuarios no podrán instalar manualmente ninguna actualización de Microsoft Windows Update en sus dispositivos. Toda actualización que resulte adecuada se instalará respetando la configuración que usted defina.

  Seleccione esta opción si desea administrar la instalación de actualizaciones en forma central.

  Podría utilizar esta opción, por ejemplo, para optimizar el cronograma de instalación de actualizaciones y evitar sobrecargas en la red. Puede programar la instalación para que se lleve a cabo fuera del horario laboral a fin de no interferir con la productividad de los usuarios.

8. Seleccione el modo de búsqueda de Windows Update:

- **Activo**

  Si selecciona esta opción, el Servidor de administración (asistido por el Agente de red) hará que el Agente de Windows Update del dispositivo cliente realice una solicitud al origen de actualizaciones (los servidores de Windows Update o WSUS). Tras ello, el Agente de red transmitirá al Servidor de administración la información que reciba del Agente de Windows Update.

  Esta opción solo tiene efecto si la tarea *Buscar vulnerabilidades y actualizaciones requeridas* tiene habilitada la opción **Conectarse al servidor de actualizaciones para actualizar los datos**.

  Esta opción está seleccionada de forma predeterminada.

- **Pasivo**

  Si selecciona esta opción, el Agente de red se comunicará periódicamente con el Servidor de administración para enviarle información sobre las actualizaciones obtenidas durante la última sincronización entre el Agente de Windows Update y el origen de actualizaciones. Si el Agente de Windows Update no se sincroniza con un origen de actualizaciones, la información sobre actualizaciones del Servidor de administración se vuelve obsoleta.

  Seleccione esta opción si desea obtener actualizaciones de la caché del origen de actualizaciones.

- **Deshabilitado**

  Si selecciona esta opción, el Servidor de administración no solicitará información sobre las actualizaciones.

  Seleccione esta opción si, por ejemplo, desea probar primero las actualizaciones en su dispositivo local.

9. Seleccione la opción **Analizar los archivos ejecutables en busca de vulnerabilidades al iniciarlos** si desea analizar los archivos ejecutables en busca de vulnerabilidades mientras los archivos se están ejecutando.

10. Asegúrese de que la edición esté bloqueada para toda la configuración que haya cambiado. De lo contrario, los cambios no se aplicarán.

11. Haga clic en **Aplicar**.

# Reparación de vulnerabilidades en el software de terceros

En esta sección, se describen las características de Kaspersky Security Center relacionadas con la reparación de vulnerabilidades en el software instalado en dispositivos administrados.

## Procedimiento: búsqueda y reparación de vulnerabilidades de software de terceros

En esta sección, se describe un escenario para buscar y reparar vulnerabilidades en dispositivos administrados que utilizan el sistema operativo Windows. Puede buscar y reparar vulnerabilidades de software en el sistema operativo y en las aplicaciones de terceros, incluidas las de Microsoft.

## Requisitos previos

- Kaspersky Security Center está desplegado en su organización.
- Hay dispositivos administrados que ejecutan Windows en su organización.
- Se requiere conexión a Internet para que el Servidor de administración realice las siguientes tareas:
  - Hacer una lista de reparaciones recomendadas para vulnerabilidades en el software de Microsoft. Los especialistas de Kaspersky crean y actualizan periódicamente esta lista.
  - Reparar vulnerabilidades en software de terceros que no sea el software de Microsoft.

## Etapas

El proceso para buscar y reparar vulnerabilidades de software se divide en etapas:

1. **Análisis en busca de vulnerabilidades en el software instalado en los dispositivos administrados**

   Para encontrar vulnerabilidades en el software instalado en los dispositivos administrados, ejecute la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Cuando se completa esta tarea, Kaspersky Security Center recibe las listas de vulnerabilidades detectadas y las actualizaciones necesarias para el software de terceros instalado en los dispositivos que especificó en las propiedades de la tarea.

   La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea automáticamente con el Asistente de inicio rápido de Kaspersky Security Center. Si no ejecutó el asistente de inicio rápido, hágalo ahora o cree la tarea manualmente.

   Instrucciones:

   - Consola de administración: Análisis de aplicaciones en busca de vulnerabilidades, Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas
   - Kaspersky Security Center Web Console: Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas, Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

2. **Analizar la lista de vulnerabilidades de software detectadas**

   Abra la lista **Vulnerabilidades de software** y decida qué vulnerabilidades desea reparar. Para ver información detallada sobre una vulnerabilidad, haga clic en el nombre de la misma en la lista. La aplicación le da acceso a estadísticas sobre el estado de cada vulnerabilidad en los dispositivos administrados.

   Instrucciones:

   - Consola de administración: visualización de vulnerabilidades de software de información, visualización de estadísticas de vulnerabilidades en dispositivos administrados
   - Kaspersky Security Center Web Console: Consultar información sobre vulnerabilidades de software, Visualización de estadísticas de vulnerabilidades en dispositivos administrados

3. **Configurar la reparación de vulnerabilidades**

   Una vez que se han detectado las vulnerabilidades de software, puede repararlas en los dispositivos administrados con las tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades* y *Reparar vulnerabilidades*.

Utilice la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para aplicar actualizaciones y reparar vulnerabilidades en las aplicaciones de terceros (incluidas las de Microsoft) instaladas en los dispositivos administrados. La tarea permite instalar múltiples actualizaciones y reparar múltiples vulnerabilidades siguiendo un conjunto de reglas. Tenga en cuenta que esta tarea se puede crear únicamente si se cuenta con una licencia para la función Administración de vulnerabilidades y parches. Para corregir vulnerabilidades de software, la a tarea utiliza actualizaciones de software recomendadas *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

La tarea *Reparar vulnerabilidades* no requiere la opción de licencia correspondiente a la función Administración de vulnerabilidades y parches. Para utilizar esta tarea, debe especificar manualmente las correcciones del usuario para las vulnerabilidades en el software de terceros que figuran en la configuración de la tarea. La tarea *Reparar vulnerabilidades* utiliza correcciones recomendadas para el software de Microsoft y correcciones de usuario para software de terceros.

Puede crear estas tareas en forma manual o a través de Asistente de reparación de vulnerabilidades, que las crea en forma automática.

Instrucciones:

- Consola de administración: selección de soluciones de usuario para vulnerabilidades en software de terceros, reparación de la vulnerabilidad en aplicaciones
- Kaspersky Security Center Web Console: Selección de soluciones de usuario para vulnerabilidades en el software de terceros, Reparación de vulnerabilidades en software de terceros, Creación de la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades

**4 Programar las tareas**

Para asegurarse de que la lista de vulnerabilidades siempre esté actualizada, defina una programación que haga que la tarea *Buscar vulnerabilidades y actualizaciones requeridas* se ejecute automáticamente de tanto en tanto. Se recomienda una frecuencia promedio de una vez a la semana.

Si creó la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede programarla para que se ejecute con igual o menor frecuencia que la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Aunque puede definir una programación para la tarea *Reparar vulnerabilidades*, tenga en cuenta que, cada vez que esta se inicie, deberá seleccionar los parches que se aplicarán al software de Microsoft o de otros desarrolladores.

Cuando programe las tareas, asegúrese de que las tareas para reparar vulnerabilidades se inicien después de que finalice la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

**5 Ignorar vulnerabilidades de software (opcional)**

Puede ignorar aquellas vulnerabilidades de software que no desee reparar en ninguno de los dispositivos administrados o en algunos dispositivos administrados específicos.

Instrucciones:

- Consola de administración: ignorar las vulnerabilidades de software
- Kaspersky Security Center Web Console: Ignorar las vulnerabilidades de software

**6 Ejecutar una tarea de reparación de vulnerabilidades**

Inicie las tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades* o *Reparar vulnerabilidad*. Cuando se complete la tarea, asegúrese de que tenga el estado *Completada correctamente* en la lista de tareas.

**7 Crear el informe sobre los resultados de la reparación de vulnerabilidades de software (opcional)**

Para ver estadísticas detalladas sobre la reparación de vulnerabilidades, genere el Informe de vulnerabilidades. El informe le indicará qué vulnerabilidades de software no se corrigieron. Ello le dará un panorama sobre la búsqueda y reparación de vulnerabilidades en el software de terceros (incluido el software de Microsoft) instalado en su organización.

Instrucciones:

- Consola de administración: Crear y ver un informe
- Kaspersky Security Center Web Console: Generar y ver un informe

8. **Revisar la configuración de la búsqueda y reparación de vulnerabilidades en el software de terceros**

   Asegúrese de haber hecho lo siguiente:

   - Obtenido y revisado la lista de vulnerabilidades de software detectadas en los dispositivos administrados.
   - Ignorado las vulnerabilidades de software si así lo deseaba.
   - Configurado la tarea para reparar vulnerabilidades.
   - Programado las tareas de encontrar y reparar vulnerabilidades de software para que comiencen secuencialmente.
   - Comprobado que se haya ejecutado la tarea para reparar vulnerabilidades de software.

### Resultados

Si creó y configuró la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, las vulnerabilidades se repararán en los dispositivos administrados automáticamente. Cuando se ejecuta, la tarea compara la lista de actualizaciones de software disponibles con las reglas especificadas en su configuración. Todas las actualizaciones de software que cumplan con los criterios especificados en las reglas se descargarán en el repositorio del Servidor de administración y se instalarán para reparar las vulnerabilidades de software.

Si creó la tarea *Reparar vulnerabilidades*, solo se corregirán las vulnerabilidades presentes en el software de Microsoft.

## Acerca de la búsqueda y reparación de vulnerabilidades de software

Kaspersky Security Center detecta y corrige vulnerabilidades de software en dispositivos administrados que ejecutan los sistemas operativos de Microsoft Windows. La solución puede detectar vulnerabilidades tanto en el sistema operativo como en aplicaciones desarrolladas por Microsoft y otros terceros.

La función de actualizaciones (incluido el suministro de actualizaciones para las firmas antivirus y la base de código) y la función de KSN pueden dejar de estar disponibles en el software en el territorio de EE. UU.

### Búsqueda de vulnerabilidades de software

Para encontrar vulnerabilidades de software, Kaspersky Security Center utiliza funciones de la base de datos de vulnerabilidades conocidas. Los especialistas de Kaspersky crean esta base de datos. Contiene distintos datos sobre cada vulnerabilidad: su descripción, su fecha de detección, su nivel de gravedad y más. Puede ver los detalles de las vulnerabilidades de software en el sitio web de Kaspersky.

Kaspersky Security Center usa la tarea *Buscar vulnerabilidades y actualizaciones requeridas* para encontrar vulnerabilidades de software.

En ciertos casos, las vulnerabilidades detectadas en un sistema operativo Microsoft Windows se pueden reparar utilizando cualquiera de los siguientes métodos:

- Instalar una actualización para el sistema operativo.
- Actualizar el sistema operativo a una versión más reciente (por ejemplo, de Windows 10 a Windows 11).

En este escenario, Kaspersky Security Center muestra dos entradas para la misma vulnerabilidad.

## Reparación de vulnerabilidades de software

Para reparar vulnerabilidades de software, Kaspersky Security Center utiliza actualizaciones de software que emiten los proveedores de software. Los metadatos de las actualizaciones de software se descargan en el repositorio del Servidor de administración después de que se ejecuten las siguientes tareas:

- *Descargar actualizaciones en el repositorio del Servidor de administración*. Esta tarea tiene como objetivo la descarga de metadatos de actualizaciones para software de Kaspersky y de terceros. Esta tarea se crea automáticamente con el asistente de inicio rápido de Kaspersky Security Center. Puede crear una tarea Descargar actualizaciones en el repositorio del Servidor de administración.
- *Sincronización con Windows Update*. Esta tarea tiene como objetivo la descarga de metadatos de actualizaciones para software de Microsoft.

Las actualizaciones de software con las que se corrigen las vulnerabilidades pueden ser paquetes de distribución completos o parches. Las actualizaciones de software diseñadas para corregir vulnerabilidades de software se denominan *reparaciones*. Las *correcciones recomendadas* son aquellas que los especialistas de Kaspersky sugieren instalar. Las *correcciones de usuario* son aquellas que los usuarios eligen instalar manualmente. Para instalar una corrección de usuario, se debe crear un paquete de instalación que contenga esta reparación.

Si no tiene la licencia de Kaspersky Security Center con la función de Administración de vulnerabilidades y parches para corregir las vulnerabilidades de software, puede usar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Esta tarea repara automáticamente varias vulnerabilidades instalando las reparaciones recomendadas. Si utiliza esta tarea, puede configurar manualmente ciertas reglas para la reparación de múltiples vulnerabilidades.

Si no tiene la licencia de Kaspersky Security Center con la función Administración de vulnerabilidades y parches para corregir las vulnerabilidades de software, puede usar la tarea *Reparar vulnerabilidades*. Mediante esta tarea, puede corregir vulnerabilidades instalando correcciones recomendadas para el software de Microsoft y correcciones de usuario para otro software de terceros.

Por seguridad, cada actualización de software de terceros que se instala con la función Administración de vulnerabilidades y parches se somete a un análisis antimalware automático con las tecnologías de Kaspersky Estas tecnologías revisan automáticamente los archivos utilizando técnicas de análisis antivirus, análisis estático, análisis dinámico, análisis de comportamiento en un entorno de pruebas y aprendizaje automático, entre otras.

Los expertos de Kaspersky no realizan análisis manuales de las actualizaciones de software de terceros que puedan instalarse mediante la función Administración de vulnerabilidades y parches. Tampoco buscan vulnerabilidades (conocidas o desconocidas) o funciones no documentadas en las actualizaciones ni las analizan de modos que no se hayan indicado en el párrafo anterior.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedirle al usuario que la cierre.

Para reparar algunas vulnerabilidades de software, deberá aceptar un contrato de licencia de usuario final (EULA) que lo faculte a instalar el software. Si se le solicita aceptar el EULA, hágalo. Si rechaza el EULA, la vulnerabilidad de software correspondiente no se reparará.

## Consulta de información sobre las vulnerabilidades de software

*Para ver una lista de las vulnerabilidades detectadas en dispositivos cliente,*

En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de la consola, seleccione la subcarpeta **Vulnerabilidades de software**.

La página muestra una lista con las vulnerabilidades detectadas en las aplicaciones de los dispositivos administrados.

*Para obtener información sobre una vulnerabilidad seleccionada,*

Seleccione **Propiedades** en el menú contextual de la vulnerabilidad.

Se abrirá la ventana Propiedades de la vulnerabilidad, con la siguiente información:

- Aplicación en la que se detectó la vulnerabilidad.
- Lista de los dispositivos en los cuales se detectó la vulnerabilidad.
- Información sobre si se reparó o no la vulnerabilidad.

*Para ver el informe sobre todas las vulnerabilidades detectadas,*

En la carpeta **Vulnerabilidades de software**, haga clic en el enlace **Ver informe de vulnerabilidades**.

Se generará un informe de vulnerabilidades de las aplicaciones instaladas en dispositivos. Puede ver este informe en el nodo con el nombre del Servidor de administración relevante si abre la pestaña **Informes**.

## Ver estadísticas de las vulnerabilidades presentes en los dispositivos administrados

Puede ver estadísticas sobre cada vulnerabilidad de software detectada en los dispositivos administrados. Las estadísticas se presentan en forma de diagrama. El diagrama muestra la cantidad de dispositivos con los siguientes estados:

- *Ignorada en: <cantidad de dispositivos>*. Este estado se asigna cuando la vulnerabilidad se desestima manualmente a través de sus propiedades.
- *Reparada en: <cantidad de dispositivos>*. Este estado se asigna cuando la tarea para reparar la vulnerabilidad se completa correctamente.
- *Reparación programada para: <cantidad de dispositivos>*. Este estado se asigna cuando ya se ha creado una tarea para reparar la vulnerabilidad, pero aún no se la ha ejecutado.

- *Parche aplicado en: <cantidad de dispositivos>*. Este estado se asigna cuando se seleccionó manualmente una actualización de software que debía, pero no pudo, reparar la vulnerabilidad.

- *Es necesario realizar un arreglo en: <cantidad de dispositivos>*. Este estado se asigna cuando la vulnerabilidad se ha reparado solo en algunos dispositivos administrados y aún debe repararse en más dispositivos administrados.

*Para ver las estadísticas de una vulnerabilidad en los dispositivos administrados:*

1. En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de la consola, seleccione la subcarpeta **Vulnerabilidades de software**.

   La página muestra una lista con las vulnerabilidades detectadas en las aplicaciones de los dispositivos administrados.

2. Seleccione una vulnerabilidad para la que desee ver las estadísticas.

   En el bloque para trabajar con un objeto seleccionado, se muestra un diagrama de los estados de vulnerabilidad. Para ver los dispositivos en los que la vulnerabilidad tenga un estado en particular, haga clic en ese estado.

## Análisis de aplicaciones en busca de vulnerabilidades

Si configuró la aplicación a través del asistente de inicio rápido, la tarea *Análisis de vulnerabilidades* se creará automáticamente. Puede ver la tarea en la carpeta **Dispositivos administrados** en la pestaña **Tareas**.

*Para crear una tarea de análisis de vulnerabilidades en aplicaciones instaladas en dispositivos cliente:*

1. En el árbol de la consola, seleccione **Avanzado** → **Administración de aplicaciones** y luego seleccione la subcarpeta **Vulnerabilidades de software**.

2. En el espacio de trabajo, seleccione **Acciones adicionales** → **Configurar análisis de vulnerabilidades**.

   Si ya existe una tarea de análisis de vulnerabilidades, se muestra la pestaña **Tareas** de la carpeta **Dispositivos administrados**, con la tarea existente seleccionada. De lo contrario, se inicia el Asistente para crear tarea de buscar vulnerabilidades y actualizaciones requeridas. Siga los pasos del asistente.

3. En la ventana **Seleccione el tipo de tarea**, seleccione **Buscar vulnerabilidades y actualizaciones necesarias**.

4. En la página **Configuración** del asistente, defina los siguientes ajustes para la tarea:

- **Buscar vulnerabilidades y actualizaciones catalogadas por Microsoft**

  Al buscar vulnerabilidades y actualizaciones, Kaspersky Security Center utiliza la información sobre las actualizaciones de Microsoft aplicables desde la fuente de actualizaciones de Microsoft, las cuales están disponibles en este momento.

  Podría deshabilitar esta opción si, por ejemplo, ha creado tareas diferentes (con configuraciones diferentes) para las actualizaciones de Microsoft y para las actualizaciones de aplicaciones de terceros.

  Esta opción está activada de forma predeterminada.

  La información sobre las actualizaciones opcionales de Microsoft Windows no se envía al Servidor de administración.

- **Conectarse al servidor de actualizaciones para actualizar los datos**

El Agente de Windows Update del dispositivo administrado se conectará al origen de actualizaciones de Microsoft. Los siguientes servidores pueden actuar como orígenes de actualizaciones de Microsoft:

- Servidor de administración de Kaspersky Security Center (consulte la configuración de la directiva del Agente de red)
- Un servidor Windows Server con Microsoft Windows Server Update Services (WSUS) que se encuentre instalado en la red de su organización
- Los servidores de actualizaciones de Microsoft

Cuando esta opción está habilitada, el Agente de Windows Update del dispositivo administrado se conecta al origen de actualizaciones de Microsoft para obtener información actualizada sobre las actualizaciones de Microsoft Windows aplicables.

Cuando esta opción está deshabilitada, el Agente de actualización de Windows del dispositivo administrado usa la información sobre las actualizaciones de Microsoft Windows aplicables que el origen de actualizaciones brindó en un momento anterior.

Conectarse al origen de actualizaciones de Microsoft puede consumir muchos recursos. Podría deshabilitar esta opción si ha configurado un esquema de conexión periódica a este origen en otra tarea o en la sección **Actualizaciones y vulnerabilidades de software** de las propiedades de la directiva del Agente de red. Si no quiere deshabilitar esta opción, para intentar que el Servidor de administración no se sobrecargue, modifique la programación de la tarea para que se la inicie en un punto aleatorio de un intervalo de 360 minutos.

Esta opción está activada de forma predeterminada.

El modo de obtener las actualizaciones deriva de combinar las siguientes opciones de configuración de la directiva del Agente de red:

- El Agente de Windows Update en un dispositivo administrado se conecta al Servidor de actualizaciones para obtener actualizaciones solo si la opción **Conectarse al servidor de actualizaciones para actualizar los datos** está activada en las propiedades de la tarea *Buscar vulnerabilidades y actualizaciones requeridas* y la opción de **Modo de búsqueda de Windows Update** está configurada como **Activo** en la configuración de la directiva del Agente de red.
- Si no necesita el Agente de red para iniciar una conexión al origen de actualizaciones de Microsoft Windows ni para descargar actualizaciones al realizar la tarea *Análisis de vulnerabilidades*, puede seleccionar la opción **Pasivo** en **Modo de búsqueda de Windows Update**, pero la opción **Conectarse al servidor de actualizaciones para actualizar los datos** debe permanecer habilitada. Así podrá ahorrar recursos y usar las actualizaciones de Windows antes recibidas para analizar las vulnerabilidades. Puede usar el modo pasivo si configura la recepción de actualizaciones de Microsoft Windows de otra manera. Si la recepción de actualizaciones de Microsoft Windows no está configurada de otra manera, no seleccione la opción **Pasivo** en **Modo de búsqueda de Windows Update** porque, en este caso, nunca recibirá información sobre las actualizaciones.
- Independientemente del estado de la opción **Conectarse al servidor de actualizaciones para actualizar los datos** (habilitado o deshabilitado), si se selecciona la opción **Modo de búsqueda de Windows Update** en **Deshabilitado**, Kaspersky Security Center no solicita ninguna información sobre actualizaciones.

- Buscar vulnerabilidades y actualizaciones catalogadas por Kaspersky para software de terceros

Si esta opción está habilitada, Kaspersky Security Center busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft) en el Registro de Windows y en las carpetas especificadas en **Especifique las rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**. Kaspersky determina el alcance de la lista de aplicaciones de terceros compatibles.

Si esta opción está deshabilitada, Kaspersky Security Center no busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros. Puede que quiera deshabilitar esta opción si utiliza tareas diferentes, con configuraciones diferentes, para las actualizaciones de Microsoft Windows y para las actualizaciones de aplicaciones de terceros.

Esta opción está activada de forma predeterminada.

- **Especifique las rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**

  Carpetas en las que Kaspersky Security Center buscará aplicaciones de terceros que requieran la instalación de actualizaciones o que tengan vulnerabilidades que deban repararse. Puede utilizar variables del sistema.

  Especifique las carpetas en las que se instalan las aplicaciones. De forma predeterminada, la lista contiene carpetas del sistema en las que se instalan la mayoría de las aplicaciones.

- **Habilitar diagnóstico avanzado**

  Si esta función está habilitada, el Agente de red escribe archivos de seguimiento, incluso si la escritura de archivos de seguimiento está deshabilitada para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center. Los datos de seguimiento se guardan en dos archivos sucesivamente; el tamaño total de ambos archivos está determinado por el valor de la opción **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando los archivos alcanzan su límite de tamaño, el Agente de red comienza a sobrescribirlos. Los archivos de seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

  Si esta función está deshabilitada, el Agente de red escribe rastreos de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center. No se guardará ningún otro dato de seguimiento.

  No es necesario que habilite la característica de diagnóstico avanzado al momento de crear una tarea. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

  Esta opción está deshabilitada de forma predeterminada.

- **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Los especialistas en soporte técnico de Kaspersky podrían pedirle que cambie el valor predeterminado si, para solucionar un problema, les remite archivos de diagnóstico avanzado con información insuficiente.

5. En la página **Configurar programación de tarea** del asistente, puede crear una programación para el inicio de la tarea. De ser necesario, configure los siguientes ajustes:

- Inicio programado:

  Seleccione y configure la programación según la cual se ejecutará la tarea.

  - Cada N horas

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

    De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

  - Cada N días

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

    De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

  - Cada N semanas

    La tarea se ejecutará periódicamente, a intervalos regulares, en el día de la semana y a la hora que especifique. Cada ejecución estará separada de la anterior por el número de semanas que indique.

    Por defecto, la tarea se ejecutará cada lunes a la hora actual del sistema.

  - Cada N minutos

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

    De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

  - Diario (no compatible con horario de verano)

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta programación no tiene en cuenta los cambios de horario estacionales. La hora de inicio de la tarea se mantendrá sin cambios incluso si el reloj se atrasa o se adelanta una hora debido al horario de verano.

    No recomendamos usar esta programación. Se la ofrece para mantener la compatibilidad con versiones anteriores de Kaspersky Security Center.

    De forma predeterminada, la tarea se iniciará todos los días a la hora actual del sistema.

  - Semanal

La tarea se ejecutará cada semana en el día y a la hora que indique.

- **Por días de la semana**

  La tarea se ejecutará periódicamente en los días de la semana y a la hora que indique.

  De manera predeterminada, la tarea se ejecutará todos los viernes a las 18:00:00.

- **Mensual**

  La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

  Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

  Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

- **Manual**

  La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

  Esta opción está seleccionada de forma predeterminada.

- **Cada mes en los días especificados de semanas seleccionadas**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  Por defecto, la hora de inicio es a las 18:00 y no se selecciona ningún día del mes.

  Tenga en cuenta que no selecciona una fecha específica en el mes, ni el número de la semana (primera, segunda semana del mes), sino el número de secuencia del día de la semana dentro de un mes. Por ejemplo, si coloca el cursor en la celda **Ma** de la **Primero** fila, significa que la tarea se ejecutará el primer martes de cada mes nuevo.

  Puede seleccionar varios días de la semana.

- **Al descargar nuevas actualizaciones al repositorio**

  La tarea se ejecuta después de descargar las actualizaciones en el repositorio. Por ejemplo, es posible que desee utilizar este programa para la tarea de encontrar vulnerabilidades y actualizaciones necesarias.

- **Ante brotes de virus**

La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

- Antivirus para estaciones de trabajo y servidores de archivos
- Antivirus para defensa del perímetro
- Antivirus para sistemas de correo

Por defecto, están seleccionados todos los tipos de aplicaciones.

En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- Al completarse otra tarea

  La tarea actual se iniciará después de que se complete otra tarea. Esta opción solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

- Ejecutar tareas no realizadas

  Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

  Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

  Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

  Esta opción está deshabilitada de forma predeterminada.

- Esperar un tiempo definido al azar antes de iniciar la tarea

Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

- Limitar el tiempo de espera a esta cantidad de minutos

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

  Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

6. En la página **Defina el nombre de la tarea** del asistente, especifique el nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).

7. En la página **Finalizar la creación de la tarea** del asistente, haga clic en el botón **Finalizar** para cerrar el asistente.

   Para que la tarea se inicie en cuanto se cierre el asistente, marque la casilla **Ejecutar la tarea al finalizar el asistente**.

Después de que termina el asistente, aparece la tarea **Buscar vulnerabilidades y actualizaciones requeridas** en la lista de tareas en la carpeta **Dispositivos administrados**, en la pestaña **Tareas**.

Además de los ajustes configurados durante el proceso de creación, la tarea tiene otras propiedades que se pueden modificar.

Cuando la tarea *Buscar vulnerabilidades y actualizaciones requeridas* finaliza, el Servidor de administración muestra una lista de vulnerabilidades encontradas en las aplicaciones instaladas en el dispositivo; también muestra todas las actualizaciones de software necesarias para solucionar las vulnerabilidades detectadas.

Si encuentra el 0x80240033 "Error del Agente de Windows Update 80240033 (" No se pudieron descargar los términos de licencia ")", puede resolver este problema a través del Registro de Windows .

El Servidor de administración no muestra la lista de actualizaciones de software requeridas cuando ejecutan dos tareas de forma secuencial: la tarea *de sincronización Realizar actualización de Windows* que tiene la opción **Descargar archivos de instalación rápida** deshabilitada, y luego la *tarea Encontrar vulnerabilidades y actualizaciones necesarias*. Para ver la lista de actualizaciones de software necesarias, debe ejecutar nuevamente la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

El Agente de red recibe información sobre cualquier actualización de Windows disponible y otras actualizaciones de productos de Microsoft desde Windows Update o el Servidor de administración, en caso de que el Servidor de administración actúe como servidor WSUS. La información se transmite cuando las aplicaciones se inician (si esta es proporcionada por la directiva) y en cada ejecución rutinaria de la tarea *Buscar vulnerabilidades y actualizaciones requeridas* en dispositivos cliente.

## Reparación de vulnerabilidades en las aplicaciones

Si seleccionó **Buscar e instalar actualizaciones requeridas** en la página **Opciones de administración de actualizaciones** del Asistente de inicio rápido, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se crea automáticamente. La tarea se muestra en el espacio de trabajo de la carpeta **Dispositivos administrados** en la pestaña **Tareas**.

De lo contrario, puede hacer lo siguiente:

- Cree una tarea para corregir vulnerabilidades instalando actualizaciones disponibles.
- Agregue una regla para reparar una vulnerabilidad a una tarea de reparación de vulnerabilidades existente.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedirle al usuario que la cierre.

### Reparar vulnerabilidades creando una tarea de reparación de vulnerabilidades

Puedes hacer lo siguiente:

- Cree una tarea para reparar múltiples vulnerabilidades que cumplan ciertas reglas.
- Seleccione una vulnerabilidad y cree una tarea para reparar esa y otras vulnerabilidades similares.

*Para reparar vulnerabilidades que cumplan ciertas reglas:*

1. En el árbol de la consola, seleccione Servidor de administración en los dispositivos para los que desea corregir vulnerabilidades.
2. En el menú **Ver** de la ventana principal de la aplicación, seleccione **Configuración de interfaz**.
3. En la ventana que se abre, marque la casilla de verificación **Mostrar Administración de vulnerabilidades y parches** y haga clic en **Aceptar**.
4. En la ventana con el mensaje de la aplicación, haga clic en **Aceptar**.
5. Reinicie la Consola de administración para que los cambios surtan efecto.
6. En el árbol de consola, seleccione la carpeta **Dispositivos administrados**.
7. En el espacio de trabajo, seleccione la pestaña **Tareas**.
8. Haga clic en el botón **Crear una tarea** para ejecutar el Asistente para crear nueva tarea. Siga los pasos del asistente.

9. En la página **Seleccione el tipo de tarea** del asistente, seleccione **Instalar actualizaciones requeridas y reparar vulnerabilidades**.

   Si la tarea no aparece, compruebe si su cuenta tiene los derechos de **Lectura**, **Modificación**, y **Ejecución** para el área funcional **Administración del sistema**: **Administración de vulnerabilidades y parches** área funcional. Sin estos derechos de acceso, no puede crear y configurar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

10. En la página **Configuración** del asistente, defina los siguientes ajustes para la tarea:

- **Elija las reglas de instalación de actualizaciones**

  Estas reglas se aplican a la instalación de actualizaciones en dispositivos cliente. Si no se especifican las reglas, la tarea no tiene nada que realizar. Para obtener información sobre las operaciones con reglas, consulte Reglas para la instalación de actualizaciones.

- **Comenzar instalación cuando se esté por reiniciar o apagar el dispositivo**

  Si esta opción está habilitada, las actualizaciones se instalarán en el momento en el que los dispositivos se reinicien o se apaguen. De lo contrario, las actualizaciones se instalarán siguiendo la programación que se defina.

  Utilice esta opción si la instalación de las actualizaciones podría afectar el rendimiento de los dispositivos.

  Esta opción está deshabilitada de forma predeterminada.

- **Instalar los componentes requeridos y generales del sistema**

  Si esta opción está habilitada, antes de que se instale una actualización, la aplicación instalará automáticamente todos los componentes generales del sistema que la actualización requiera para instalarse (los llamados "requisitos previos"). Una actualización podría requerir, por ejemplo, que esté instalada cierta actualización del sistema operativo.

  Si esta opción está deshabilitada, posiblemente tenga que instalar los requisitos previos manualmente.

  Esta opción está deshabilitada de forma predeterminada.

- **Permitir la instalación de versiones nuevas de aplicaciones durante las actualizaciones**

  Si esta opción está habilitada, las actualizaciones podrán cambiar la versión del software actualizado por una más reciente.

  Si esta opción está deshabilitada, los cambios de versión no estarán permitidos. Para instalar una versión más reciente de una aplicación, deberá usar una tarea diferente o proceder en forma manual. Podría usar esta opción si, por ejemplo, desea evaluar el cambio de versión en una infraestructura de prueba o si sabe que la versión más reciente no es compatible con la infraestructura de su empresa.

  Esta opción está activada de forma predeterminada.

  Los cambios de versión pueden ocasionar problemas de funcionamiento en las aplicaciones dependientes instaladas en los dispositivos cliente.

- **Descargar actualizaciones en el dispositivo sin instalarlas**

Si esta opción está habilitada, la aplicación descargará las actualizaciones disponibles en los dispositivos, pero no las instalará automáticamente. Podrá instalar las actualizaciones descargadas manualmente.

Las actualizaciones de Microsoft se descargan en el sistema de almacenamiento de Windows. Las actualizaciones para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky ni Microsoft) se descargan en la carpeta especificada en el campo **Descargar actualizaciones en**.

Si esta opción está deshabilitada, las actualizaciones se instalarán en los dispositivos automáticamente.

Esta opción está deshabilitada de forma predeterminada.

- **Descargar actualizaciones en**

  Esta carpeta se utiliza para descargar las actualizaciones para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky ni Microsoft).

- **Habilitar diagnóstico avanzado**

  Si esta función está habilitada, el Agente de red escribe archivos de seguimiento, incluso si la escritura de archivos de seguimiento está deshabilitada para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center. Los datos de seguimiento se guardan en dos archivos sucesivamente; el tamaño total de ambos archivos está determinado por el valor de la opción **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando los archivos alcanzan su límite de tamaño, el Agente de red comienza a sobrescribirlos. Los archivos de seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

  Si esta función está deshabilitada, el Agente de red escribe rastreos de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center. No se guardará ningún otro dato de seguimiento.

  No es necesario que habilite la característica de diagnóstico avanzado al momento de crear una tarea. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

  Esta opción está deshabilitada de forma predeterminada.

  - **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

    El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Los especialistas en soporte técnico de Kaspersky podrían pedirle que cambie el valor predeterminado si, para solucionar un problema, les remite archivos de diagnóstico avanzado con información insuficiente.

11. En la página **Seleccione la opción de reinicio del sistema operativo** del asistente, seleccione la acción a realizar cuando el sistema operativo de los dispositivos cliente deba reiniciarse después de la operación:

- **No reiniciar el dispositivo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

- **Reiniciar el dispositivo**

  Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

  Esta opción está seleccionada de forma predeterminada.

  - **Repetir solicitud cada (min)**

    Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

    Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

    Si no habilita esta opción, la solicitud se mostrará una sola vez.

  - **Reiniciar después de (min)**

    Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

    Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de aplicaciones en sesiones bloqueadas**

Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

Esta opción está deshabilitada de forma predeterminada.

12. En la página **Configurar programación de tarea** del asistente, puede crear una programación para el inicio de la tarea. De ser necesario, configure los siguientes ajustes:

- Inicio programado:

  Seleccione y configure la programación según la cual se ejecutará la tarea.

  - Cada N horas

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

    De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

  - Cada N días

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

    De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

  - Cada N semanas

    La tarea se ejecutará periódicamente, a intervalos regulares, en el día de la semana y a la hora que especifique. Cada ejecución estará separada de la anterior por el número de semanas que indique.

    Por defecto, la tarea se ejecutará cada lunes a la hora actual del sistema.

  - Cada N minutos

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

    De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

  - Diario (no compatible con horario de verano)

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta programación no tiene en cuenta los cambios de horario estacionales. La hora de inicio de la tarea se mantendrá sin cambios incluso si el reloj se atrasa o se adelanta una hora debido al horario de verano.

    No recomendamos usar esta programación. Se la ofrece para mantener la compatibilidad con versiones anteriores de Kaspersky Security Center.

    De forma predeterminada, la tarea se iniciará todos los días a la hora actual del sistema.

  - Semanal

La tarea se ejecutará cada semana en el día y a la hora que indique.

- **Por días de la semana**

  La tarea se ejecutará periódicamente en los días de la semana y a la hora que indique.

  De manera predeterminada, la tarea se ejecutará todos los viernes a las 18:00:00.

- **Mensual**

  La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

  Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

  Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

- **Manual**

  La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

  Esta opción está seleccionada de forma predeterminada.

- **Cada mes en los días especificados de semanas seleccionadas**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  Por defecto, la hora de inicio es a las 18:00 y no se selecciona ningún día del mes.

  Tenga en cuenta que no selecciona una fecha específica en el mes, ni el número de la semana (primera, segunda semana del mes), sino el número de secuencia del día de la semana dentro de un mes. Por ejemplo, si coloca el cursor en la celda Tu de la Primera fila, significa que la tarea se ejecutará el primer martes de cada mes nuevo.**MaPrimero**

  Puede seleccionar varios días de la semana.

- **Ante brotes de virus**

  La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para defensa del perímetro
  - Antivirus para sistemas de correo

  Por defecto, están seleccionados todos los tipos de aplicaciones.

  En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- Al completarse otra tarea

  La tarea actual se iniciará después de que se complete otra tarea. Esta opción solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

- Ejecutar tareas no realizadas

  Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

  Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

  Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

  Esta opción está deshabilitada de forma predeterminada.

- Esperar un tiempo definido al azar antes de iniciar la tarea

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

- Limitar el tiempo de espera a esta cantidad de minutos

Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

13. En la página **Defina el nombre de la tarea** del asistente, especifique el nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).

14. En la página **Finalizar la creación de la tarea** del asistente, haga clic en el botón **Finalizar** para cerrar el asistente.

    Para que la tarea se inicie en cuanto se cierre el asistente, marque la casilla **Ejecutar la tarea al finalizar el asistente**.

Después de que el asistente termina su operación, se crea la tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades** y se la muestra en la carpeta **Tareas**.

Además de los ajustes configurados durante el proceso de creación, la tarea tiene otras propiedades que se pueden modificar.

Si los resultados de la tarea contienen el error 0x80240033 "Error del Agente de Windows Update 80240033 (" No se pudieron descargar los términos de licencia "), puede resolver este problema a través del Registro de Windows .

*Para corregir una vulnerabilidad específica y otras similares:*

1. En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de la consola, seleccione la subcarpeta **Vulnerabilidades de software**.

2. Seleccione la vulnerabilidad que desee corregir.

3. Haga clic en el botón **Ejecutar el Asistente de reparación de vulnerabilidades**.

   Se iniciará el Asistente de reparación de vulnerabilidades.

   Las funciones del Asistente de reparación de vulnerabilidades solo están disponibles con la licencia de la Administración de vulnerabilidades y parches.

   Siga los pasos del asistente.

4. En la ventana **Buscar tareas de reparación de vulnerabilidades existentes**, configure los siguientes parámetros:

   - **Mostrar solo las tareas que permitan reparar esta vulnerabilidad**

     Si esta opción está habilitada, el Asistente de reparación de vulnerabilidades busca las tareas existentes que reparan la vulnerabilidad seleccionada.

     Si esta opción está deshabilitada o si la búsqueda no produce tareas aplicables, el Asistente de reparación de vulnerabilidades le solicita crear una regla o tarea para reparar la vulnerabilidad.

     Esta opción está activada de forma predeterminada.

   - **Aprobar actualizaciones que reparen esta vulnerabilidad**

     Las actualizaciones que reparen una vulnerabilidad serán aprobadas para su instalación. Habilite esta opción si algunas de las reglas aplicadas para la instalación de actualizaciones solo permiten instalar actualizaciones aprobadas.

     Esta opción está deshabilitada de forma predeterminada.

5. Si elige buscar tareas de reparación de vulnerabilidades existentes y si la búsqueda recupera algunas tareas, puede ver las propiedades de estas tareas o iniciarlas manualmente. No se requieren más acciones.

   De lo contrario, haga clic en el botón **Nueva tarea de reparación de vulnerabilidades**.

6. Seleccione el tipo de regla de reparación de vulnerabilidades que se agregará a la nueva tarea y luego haga clic en el botón **Finalizar**.

7. Haga su elección en la ventana que aparece sobre la instalación de todas las actualizaciones de aplicaciones anteriores. Haga clic en **Sí** si está de acuerdo con la instalación de versiones sucesivas de la aplicación de forma incremental si es necesario para instalar las actualizaciones seleccionadas. Haga clic en **No** si desea actualizar las aplicaciones de forma sencilla, sin necesidad de instalar versiones sucesivas. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

   El Asistente de creación de tareas de instalación de actualizaciones y reparación de vulnerabilidades se inicia. Siga los pasos del asistente.

8. En la página **Seleccione la opción de reinicio del sistema operativo** del asistente, seleccione la acción a realizar cuando el sistema operativo de los dispositivos cliente deba reiniciarse después de la operación:

- **No reiniciar el dispositivo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

- **Reiniciar el dispositivo**

  Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

  Esta opción está seleccionada de forma predeterminada.

  - **Repetir solicitud cada (min)**

    Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

    Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

    Si no habilita esta opción, la solicitud se mostrará una sola vez.

  - **Reiniciar después de (min)**

    Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

    Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de aplicaciones en sesiones bloqueadas**

Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

Esta opción está deshabilitada de forma predeterminada.

9. En la página **Seleccionar dispositivos a los que se asignará la tarea** del asistente, seleccione una de las siguientes opciones:

- **Seleccionar dispositivos de la red detectados por el Servidor de administración**

  La tarea se asignará a ciertos dispositivos específicos. Estos pueden ser tanto dispositivos asignados a grupos de administración como dispositivos no asignados.

  Podría usar esta opción para, por ejemplo, una tarea que instale el Agente de red en los dispositivos que no estén asignados a un grupo de administración.

- **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**

  Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

  Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.

- **Asignar tarea a una selección de dispositivos**

  La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

  Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

- **Asignar tarea a un grupo de administración**

  La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

  Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

  Si la tarea se asigna a un grupo de administración, la pestaña **Seguridad** no se mostrará en la ventana de propiedades de la tarea; esto se debe a que las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

10. En la página **Configurar programación de tarea** del asistente, puede crear una programación para el inicio de la tarea. De ser necesario, configure los siguientes ajustes:

- Inicio programado:

  Seleccione y configure la programación según la cual se ejecutará la tarea.

  - Cada N horas

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

    De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

  - Cada N días

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

    De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

  - Cada N semanas

    La tarea se ejecutará periódicamente, a intervalos regulares, en el día de la semana y a la hora que especifique. Cada ejecución estará separada de la anterior por el número de semanas que indique.

    Por defecto, la tarea se ejecutará cada lunes a la hora actual del sistema.

  - Cada N minutos

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

    De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

  - Diario (no compatible con horario de verano)

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta programación no tiene en cuenta los cambios de horario estacionales. La hora de inicio de la tarea se mantendrá sin cambios incluso si el reloj se atrasa o se adelanta una hora debido al horario de verano.

    No recomendamos usar esta programación. Se la ofrece para mantener la compatibilidad con versiones anteriores de Kaspersky Security Center.

    De forma predeterminada, la tarea se iniciará todos los días a la hora actual del sistema.

  - Semanal

La tarea se ejecutará cada semana en el día y a la hora que indique.

- **Por días de la semana**

  La tarea se ejecutará periódicamente en los días de la semana y a la hora que indique.

  De manera predeterminada, la tarea se ejecutará todos los viernes a las 18:00:00.

- **Mensual**

  La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

  Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

  Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

- **Manual**

  La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

  Esta opción está seleccionada de forma predeterminada.

- **Cada mes en los días especificados de semanas seleccionadas**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  Por defecto, la hora de inicio es a las 18:00 y no se selecciona ningún día del mes.

  Tenga en cuenta que no selecciona una fecha específica en el mes, ni el número de la semana (primera, segunda semana del mes), sino el número de secuencia del día de la semana dentro de un mes. Por ejemplo, si coloca el cursor en la celda **Ma** de la **Primero** fila, significa que la tarea se ejecutará el primer martes de cada mes nuevo.

  Puede seleccionar varios días de la semana.

- **Ante brotes de virus**

  La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para defensa del perímetro
  - Antivirus para sistemas de correo

  Por defecto, están seleccionados todos los tipos de aplicaciones.

  En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- **Al completarse otra tarea**

  La tarea actual se iniciará después de que se complete otra tarea. Esta opción solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

- **Ejecutar tareas no realizadas**

  Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

  Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

  Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

  Esta opción está deshabilitada de forma predeterminada.

- **Esperar un tiempo definido al azar antes de iniciar la tarea**

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

- **Limitar el tiempo de espera a esta cantidad de minutos**

Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

11. En la página **Defina el nombre de la tarea** del asistente, especifique el nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).

12. En la página **Finalizar la creación de la tarea** del asistente, haga clic en el botón **Finalizar** para cerrar el asistente.

    Para que la tarea se inicie en cuanto se cierre el asistente, marque la casilla **Ejecutar la tarea al finalizar el asistente**.

Cuando el asistente termina, se crea la tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades** y se muestra en la carpeta **Tareas**.

Además de los ajustes configurados durante el proceso de creación, la tarea tiene otras propiedades que se pueden modificar.

## Reparar una vulnerabilidad agregando una regla a una tarea de reparación de vulnerabilidades existente

*Para reparar una vulnerabilidad agregando una regla a una tarea de reparación de vulnerabilidades existente:*

1. En la carpeta **Avanzado → Administración de aplicaciones** del árbol de la consola, seleccione la subcarpeta **Vulnerabilidades de software**.

2. Seleccione la vulnerabilidad que desee corregir.

3. Haga clic en el botón **Ejecutar el Asistente de reparación de vulnerabilidades**.

   Se iniciará el Asistente de reparación de vulnerabilidades.

   Las funciones del Asistente de reparación de vulnerabilidades solo están disponibles con la licencia de la Administración de vulnerabilidades y parches.

   Siga los pasos del asistente.

4. En la ventana **Buscar tareas de reparación de vulnerabilidades existentes**, configure los siguientes parámetros:

   - **Mostrar solo las tareas que permitan reparar esta vulnerabilidad**

     Si esta opción está habilitada, el Asistente de reparación de vulnerabilidades busca las tareas existentes que reparan la vulnerabilidad seleccionada.

     Si esta opción está deshabilitada o si la búsqueda no produce tareas aplicables, el Asistente de reparación de vulnerabilidades le solicita crear una regla o tarea para reparar la vulnerabilidad.

     Esta opción está activada de forma predeterminada.

   - **Aprobar actualizaciones que reparen esta vulnerabilidad**

     Las actualizaciones que reparen una vulnerabilidad serán aprobadas para su instalación. Habilite esta opción si algunas de las reglas aplicadas para la instalación de actualizaciones solo permiten instalar actualizaciones aprobadas.

     Esta opción está deshabilitada de forma predeterminada.

5. Si elige buscar tareas de reparación de vulnerabilidades existentes y si la búsqueda recupera algunas tareas, puede ver las propiedades de estas tareas o iniciarlas manualmente. No se requieren más acciones.

   De lo contrario, haga clic en el botón **Agregar regla de reparación a una tarea existente**.

6. Seleccione la tarea a la que desea agregar una regla y luego haga clic en el botón **Agregar regla**.

   Además, puede ver las propiedades de las tareas existentes, iniciarlas manualmente o crear una nueva tarea.

7. Seleccione el tipo de regla que se agregará a la tarea seleccionada y luego haga clic en el botón **Finalizar**.

8. Haga su elección en la ventana que aparece sobre la instalación de todas las actualizaciones de aplicaciones anteriores. Haga clic en **Sí** si está de acuerdo con la instalación de versiones sucesivas de la aplicación de forma incremental si es necesario para instalar las actualizaciones seleccionadas. Haga clic en **No** si desea actualizar las aplicaciones de forma sencilla, sin necesidad de instalar versiones sucesivas. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

Se agrega una nueva regla para reparar la vulnerabilidad a la tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades**.

## Corrección de vulnerabilidades en una red aislada

En esta sección, se describen los pasos que le permitirán reparar vulnerabilidades de software de terceros en dispositivos administrados que se encuentren conectados a servidores de administración sin acceso a Internet.

## Procedimiento: reparar vulnerabilidades en el software de terceros

Puede instalar actualizaciones y corregir vulnerabilidades en el software de terceros instalado en los dispositivos administrados de una red aislada. En una red aislada, los dispositivos administrados (y el Servidor de administración a los que esos dispositivos están conectados) no tienen acceso a Internet. Para reparar vulnerabilidades en una red de este tipo, se necesita contar con un Servidor de administración que tenga conexión a Internet. El Servidor con acceso a Internet se utiliza para descargar parches (actualizaciones requeridas), que luego se transmiten al Servidor de administración de la red aislada.

Kaspersky Security Center no puede descargar actualizaciones para el software de Microsoft instalado en servidores de administración aislados; solo puede descargar actualizaciones para software de otros terceros, que hayan sido publicadas por los desarrolladores de esas aplicaciones.

Si desea saber cómo funciona el proceso de reparación de vulnerabilidades en una red aislada, consulte la descripción y el esquema del proceso.

### Requisitos previos

Antes de comenzar, haga lo siguiente:

1. Asigne un dispositivo para conectarse a Internet y descargar parches. Este dispositivo se contará como el Servidor de administración con acceso a Internet.
2. Instale Kaspersky Security Center (versión 14 como mínimo) en los siguientes dispositivos:
   - El dispositivo del primer punto, que actuará como Servidor de administración con acceso a Internet
   - Los dispositivos aislados, que actuarán como servidores de administración aislados de Internet (en adelante, se usará el término "servidores de administración aislados" para referirse a estos dispositivos)
3. Asegúrese de que cada Servidor de administración tenga suficiente espacio en disco para descargar y almacenar actualizaciones y parches.

### Etapas

A continuación, se enumeran las etapas del proceso para instalar actualizaciones y reparar vulnerabilidades en el software de terceros instalado en dispositivos administrados por servidores de administración aislados:

1. **Configuración del Servidor de administración con acceso a Internet**

   Prepare su Servidor de administración con acceso a Internet para administrar las solicitudes de actualizaciones de software de terceros requeridas y para descargar parches.

2. **Configuración de los servidores de administración aislados**

   Prepare los servidores de administración aislados para que, de manera periódica, generen listas con las actualizaciones que requieran y para que puedan procesar los parches que descargue el Servidor de administración con acceso a Internet. Una vez configurados, los servidores de administración aislados ya no intentarán descargar parches de Internet. En cambio, obtendrán sus actualizaciones de los parches.

3. **Transferencia de los parches e instalación de las actualizaciones en los servidores de administración aislados**

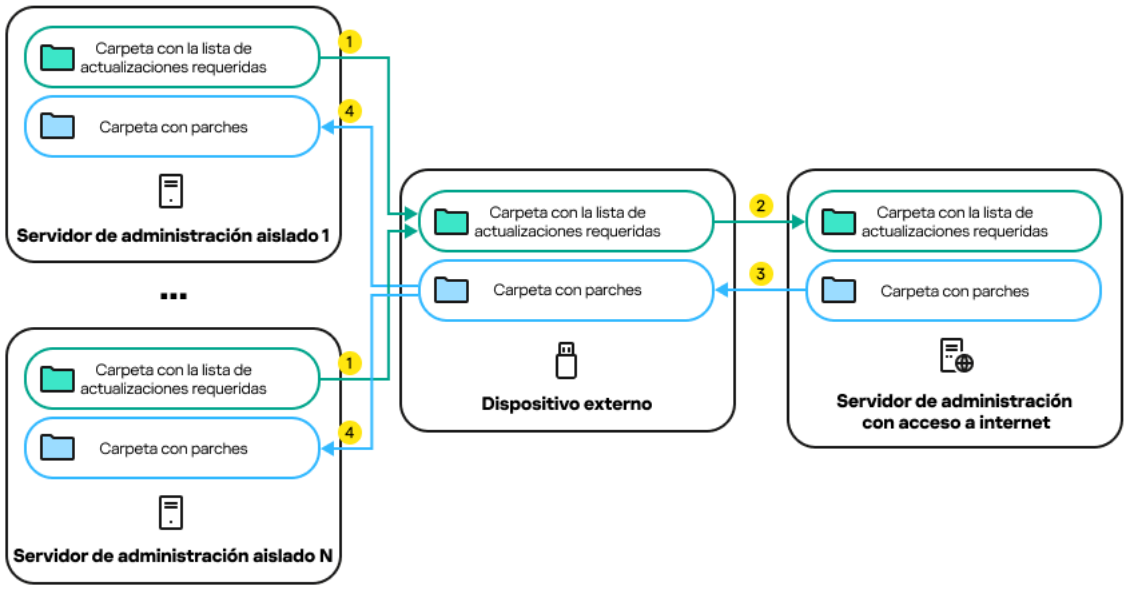
Una vez que los servidores estén configurados, podrá transmitir las listas de actualizaciones requeridas y los parches correspondientes entre el Servidor de administración con acceso a Internet y los servidores de administración aislados. Completado este intercambio, las actualizaciones contenidas en los parches se instalarán en los dispositivos administrados mediante la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

## Resultados

Como resultado, las actualizaciones para el software de terceros se transmitirán a los servidores de administración aislados y se instalarán en los dispositivos administrados conectados a los mismos a través de Kaspersky Security Center. Solo tendrá que configurar los servidores de administración una vez. Tras completar la configuración, podrá obtener las actualizaciones requeridas con la frecuencia que resulte necesaria (por ejemplo, una vez al día o varias veces al día).

## Acerca de la reparación de vulnerabilidades en el software de terceros en una red aislada

En la siguiente imagen, se describe y se grafica el proceso que permite reparar vulnerabilidades de software de terceros en una red aislada. Este proceso puede llevarse a cabo periódicamente.




Transmisión de parches y de la lista de actualizaciones requeridas entre los servidores de administración aislados y el Servidor de administración con acceso a Internet

Cada Servidor de administración aislado de Internet (denominado, en lo sucesivo, "Servidor de administración aislado") genera una lista con las actualizaciones requeridas por los dispositivos administrados que a él se encuentran conectados. La lista de actualizaciones requeridas se almacena en una carpeta específica y presenta un conjunto de archivos binarios. El nombre de cada archivo contiene el identificador del parche con la actualización requerida. Cada archivo de la lista apunta, por ende, a un parche en particular.

La lista de actualizaciones requeridas se transfiere del Servidor de administración aislado al Servidor de administración designado con acceso a Internet utilizando un dispositivo externo. Completada la transferencia, el Servidor de administración designado descarga los parches pertinentes de Internet y los pone en una carpeta separada.

Una vez que los parches pertinentes se han descargado a la carpeta específicamente creada para ellos, se los transfiere a cada Servidor de administración aislado del que se tomó una lista de actualizaciones requeridas. Los parches se guardan en una carpeta creada especialmente para ellos en el Servidor de administración aislado. Luego de esto, se ejecuta la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para instalar los parches y las actualizaciones en los dispositivos administrados conectados a los servidores de administración aislados.

## Configurar el Servidor de administración con acceso a Internet para reparar vulnerabilidades en una red aislada

Para prepararse para corregir vulnerabilidades y transmitir parches en una red aislada, configure primero el Servidor de administración con acceso a Internet y luego configure los servidores de administración aislados.

*Para configurar el Servidor de administración con acceso a Internet:*

1. Cree dos carpetas en el disco en el que esté instalado el Servidor de administración:

   - Una carpeta para almacenar la lista de actualizaciones requeridas
   - Una carpeta para los parches

   Puedes darles el nombre que desee a estas carpetas.

2. Otorgue el permiso "Modificar"Й al grupo KLAdmins para las carpetas que acaba de crear. Utilice para ello las herramientas administrativas que vienen incluidas en el sistema operativo.

3. Utilice la utilidad klscflag para escribir las rutas a las carpetas en las propiedades del Servidor de administración.

   Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada es <Disk>:\Archivos de programa(x86)\Kaspersky Lab\Kaspersky Security Center.

4. Ingrese los siguientes comandos en el símbolo del sistema de Windows:

   - Para establecer la ruta a la carpeta de parches, ingrese lo siguiente:
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<ruta a la carpeta>"`
   - Para establecer la ruta a la carpeta para la lista de actualizaciones requeridas, haga lo siguiente:
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<ruta a la carpeta>"`

   Ejemplo: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "C:\<carpeta de parches>"`

5. Si es necesario, use la utilidad klscflag para especificar la frecuencia con la que el Servidor de administración deberá buscar nuevas solicitudes de parches:
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v<valor en segundos>`

   De manera predeterminada, el valor es 120 segundos.

   Ejemplo: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 150`

6. Cree la tarea *Buscar vulnerabilidades y actualizaciones requeridas* a fin de obtener información sobre los parches para el software de terceros instalado en los dispositivos administrados. A continuación, programe la tarea.

7. Cree la tarea *Reparar vulnerabilidades* a fin de indicar qué parches se utilizarán para reparar vulnerabilidades en el software de terceros. A continuación, programe la tarea.

   Ejecute las tareas de forma manual si no quiere esperar al siguiente inicio programado. El orden en que se inician las tareas es importante. La tarea *Reparar vulnerabilidades* debe ejecutarse después de finalizada la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

8. Reinicie el servicio del Servidor de administración.

El Servidor de administración con acceso a Internet queda listo para descargar y transmitir actualizaciones a sus servidores de administración aislados. Antes de comenzar a corregir vulnerabilidades, deberá configurar los servidores de administración aislados.

## Configuración de servidores de administración aislados para corregir vulnerabilidades en una red aislada

Cuando termine de configurar el Servidor de administración con acceso a Internet, realice en cada Servidor de administración aislado los siguientes preparativos, que le permitirán corregir vulnerabilidades e instalar actualizaciones en los dispositivos administrados conectados a los mismos.

*Para configurar los servidores de administración aislados, realice las siguientes acciones en cada Servidor de administración:*

1. Active una clave de licencia para la función Administración de vulnerabilidades y parches (VAPM).

2. Cree dos carpetas en el disco en el que esté instalado el Servidor de administración:

   - La carpeta en la que aparecerá la lista de actualizaciones requeridas
   - Una carpeta para los parches

   Puedes darles el nombre que desee a estas carpetas.

3. Otorgue el permiso Modificar al grupo *KL Admins* para las carpetas que acaba de crear. Utilice para ello las herramientas administrativas que vienen incluidas en el sistema operativo.

4. Utilice la utilidad klscflag para escribir las rutas a las carpetas en las propiedades del Servidor de administración.

   Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada es <Disk>:\Archivos de programa(x86)\Kaspersky Lab\Kaspersky Security Center.

5. Ingrese los siguientes comandos en el símbolo del sistema de Windows:

   - Para establecer la ruta a la carpeta de parches, ingrese lo siguiente:
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<ruta a la carpeta>"`
   - Para establecer la ruta a la carpeta para la lista de actualizaciones requeridas, ingrese lo siguiente:
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<ruta a la carpeta>"`

   Ejemplo: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "C:\<carpeta de parches>"`

6. Si es necesario, use la utilidad klscflag para especificar la frecuencia con la que el Servidor de administración aislado buscará nuevos parches:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <valor en segundos>`

   De manera predeterminada, el valor es 120 segundos.

   Ejemplo: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 150`

7. Si es necesario, use la utilidad klscflag para calcular los hashes SHA256 de los parches:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1`

   Al utilizar este comando, sabrá si los parches sufrieron cambios al transferirse al Servidor de administración aislado. El comando también le dará la certeza de que los parches con actualizaciones requeridas recibidos son los correctos.

   De manera predeterminada, Kaspersky Security Center no calcula los hashes SHA256 de los parches. Si habilita esta opción, cuando el Servidor de administración aislado reciba parches, Kaspersky Security Center calculará los valores hash de los mismos y comparará el resultado con los valores hash almacenados en la base de datos del Servidor de administración. Si los hashes calculados no coinciden con los de la base de datos, verá un error y deberá reemplazar los parches problemáticos.

8. Cree la tarea *Buscar vulnerabilidades y actualizaciones requeridas* a fin de obtener información sobre los parches para el software de terceros instalado en los dispositivos administrados y, a continuación, programe la tarea.

9. Cree la tarea *Reparar vulnerabilidades* a fin de indicar qué parches se utilizarán para reparar vulnerabilidades en el software de terceros. A continuación, programe la tarea.

   Ejecute las tareas de forma manual si no quiere esperar al siguiente inicio programado. El orden en que se inician las tareas es importante. La tarea *Reparar vulnerabilidades* debe ejecutarse después de finalizada la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

10. Reinicie el servicio del Servidor de administración.

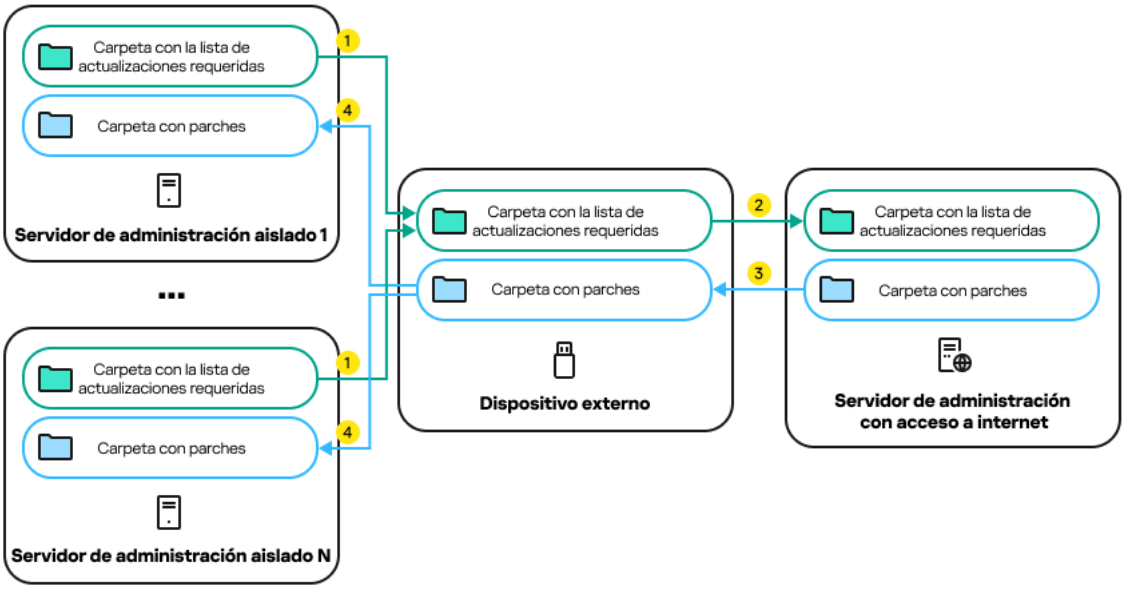
Una vez que haya configurado todos sus servidores de administración, podrá transmitir las listas de actualizaciones requeridas y los parches correspondientes para reparar vulnerabilidades en el software de terceros instalado en los dispositivos administrados de la red aislada.

## Transmitir parches e instalar actualizaciones en una red aislada

Una vez que haya configurado los servidores de administración, podrá transferir los parches que contengan las actualizaciones requeridas del Servidor de administración con acceso a Internet a los servidores de administración aislados. Las actualizaciones pueden transmitirse e instalarse con la frecuencia que se necesite (por ejemplo, una o más veces al día).

Para transferir los parches y la lista de actualizaciones requeridas entre sus servidores de administración, necesitará un dispositivo externo (por ejemplo, una unidad de almacenamiento extraíble). Asegúrese de que este dispositivo tenga espacio libre suficiente para almacenar los parches descargados.

En la siguiente imagen, se describe y se grafica el proceso según el cual se transmiten los parches y la lista de actualizaciones requeridas:




Transmisión de parches y de la lista de actualizaciones requeridas entre los servidores de administración aislados y el Servidor de administración con acceso a Internet

*Para instalar actualizaciones y reparar vulnerabilidades en dispositivos administrados conectados a servidores de administración aislados, haga lo siguiente:*

1. Inicie la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* si no se encuentra en ejecución.

2. Conecte el dispositivo externo a cualquier Servidor de administración aislado.

3. Cree dos carpetas en el dispositivo externo: una para la lista de actualizaciones requeridas y otra para los parches. Puedes darles el nombre que desee a estas carpetas.

   Si ya había creado estas carpetas, vacíelas.

4. Copie la lista de actualizaciones requeridas de cada Servidor de administración aislado y péguela en el dispositivo externo, en la carpeta que creó para la lista de actualizaciones requeridas.

   Debe juntar las listas de todos los servidores de administración aislados en una sola carpeta. Cuando termine con este paso, la carpeta contendrá archivos binarios con los identificadores de los parches requeridos por todos los servidores de administración aislados.

5. Conecte el dispositivo externo al Servidor de administración con acceso a Internet.

6. Copie la lista de actualizaciones requeridas del dispositivo externo y péguela en la carpeta que creó para la lista de actualizaciones requeridas en el Servidor de administración con acceso a Internet.

   Los parches necesarios se descargarán de Internet automáticamente y se guardarán en la carpeta de parches del Servidor de administración. El proceso puede llevar varias horas.

7. Asegúrese de descargar todos los parches necesarios. Para ello, puede realizar una de las acciones siguientes:

   - Revise la carpeta y busque los parches en el Servidor de administración con acceso a Internet. Verifique que todos los parches nombrados en la lista de actualizaciones requeridas se hayan descargado a la carpeta necesaria. Esto es más conveniente si se requiere una cantidad pequeña de parches.

   - Prepare un script especial, por ejemplo, un script de shell. Si obtiene una gran cantidad de parches, será difícil comprobar por sí mismo que se descargaron todos los parches. En casos así, es mejor automatizar la comprobación.

8. Copie los parches del Servidor de administración con acceso a Internet y péguelos en la carpeta que creó para tal fin en el dispositivo externo.

9. Transfiera los parches a todos los servidores de administración aislados. Coloque los parches en una carpeta creada para ellos.

Como resultado de estas instrucciones, cada Servidor de administración aislado creará una lista con las actualizaciones requeridas por los dispositivos administrados que a él se encuentren conectados. Cuando el Servidor de administración con acceso a Internet reciba la lista de actualizaciones requeridas, descargará los parches correspondientes de Internet. Cuando estos parches aparezcan en los servidores de administración aislados, serán procesados por la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Con ello, se instalarán las actualizaciones pertinentes en los dispositivos administrados y se corregirán las vulnerabilidades presentes en el software de terceros.

No reinicie el dispositivo en el que esté instalado el Servidor de administración mientras se esté ejecutando la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Tampoco inicie la tarea *Copia de seguridad de los datos del Servidor de administración*, pues esta dará lugar a un reinicio. Si se reinicia el dispositivo, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se interrumpirá y las actualizaciones no se instalarán. Si esta tarea se detiene, ejecútela otra vez manualmente o aguarde a que ocurra el siguiente inicio programado.

## Deshabilitar la opción para transmitir parches e instalar actualizaciones en una red aislada

Puede deshabilitar la opción de transmisión de parches en aquellos servidores de administración aislados que, por ejemplo, ya no planee tener en una red aislada. De esta forma, puede reducir la cantidad de parches y el tiempo para descargarlos.

*Para deshabilitar la opción de transmisión de parches en servidores de administración aislados:*

1. Si ya no quiere tener ningún Servidor de administración aislado, en las propiedades del Servidor de administración con acceso a Internet, elimine las rutas a las carpetas utilizadas para los parches y para la lista de actualizaciones requeridas. Si piensa mantener algunos servidores de administración en una red aislada, omita este paso.

   Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada es <Disk>:\Archivos de programa(x86)\Kaspersky Lab\Kaspersky Security Center.

   Ingrese los siguientes comandos en el símbolo del sistema:

   - Para eliminar la ruta a la carpeta utilizada para los parches:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```
   - Para eliminar la ruta a la carpeta utilizada para la lista de actualizaciones requeridas:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
     ```

2. Si eliminó las rutas de las carpetas en el Servidor de administración con acceso a Internet, reinicie el servicio del Servidor de administración.

3. En las propiedades de cada Servidor de administración que ya no quiera tener aislado, elimine las rutas a las carpetas utilizadas para los parches y para la lista de actualizaciones requeridas.

   Ingrese los siguientes comandos en el símbolo del sistema de Windows, usando derechos de administrador:

   - Para eliminar la ruta a la carpeta utilizada para los parches:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
     ```
   - Para eliminar la ruta a la carpeta utilizada para la lista de actualizaciones requeridas:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
     ```

4. Reinicie el servicio de cada Servidor de administración en el que realice la eliminación de rutas.

Si reconfiguró el Servidor de administración con acceso a Internet, dejará de recibir parches a través de Kaspersky Security Center. Si reconfiguró solo algunos servidores de administración aislados (porque, por ejemplo, piensa mantener algunos servidores aislados), recibirá parches únicamente para los servidores de administración que sigan estando aislados.

Si posteriormente necesitara reparar vulnerabilidades en los servidores aislados que deshabilitó, deberá volver a configurar tanto esos servidores de administración como el Servidor de administración con acceso a Internet.

## Ignorar vulnerabilidades de software

Puede ignorar las vulnerabilidades de software que no desee reparar. Hay distintos motivos para ignorar una vulnerabilidad de software, por ejemplo:

- no considera que la vulnerabilidad de software sea de extrema importancia para su organización;
- entiende que, al reparar la vulnerabilidad, se pondrían en riesgo los datos vinculados al software vulnerable;
- sabe que la vulnerabilidad de software no es un riesgo para la red de su organización porque utiliza otras medidas para proteger sus dispositivos administrados.

Puede ignorar una vulnerabilidad de software en todos los dispositivos administrados o solo en los dispositivos administrados que usted seleccione.

*Para ignorar una vulnerabilidad de software en todos los dispositivos administrados:*

1. En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de la consola, seleccione la subcarpeta **Vulnerabilidades de software**.

   El espacio de trabajo de la carpeta muestra una lista de las vulnerabilidades que detecta el Agente de red en aplicaciones instaladas en dispositivos.

2. Seleccione la vulnerabilidad que desee ignorar.

3. Seleccione **Propiedades** en el menú contextual de la vulnerabilidad.

   Se abre la ventana de propiedades de la vulnerabilidad.

4. En la sección **General**, elija la opción **Ignorar vulnerabilidad**.

5. Haga clic en **Aceptar**.

   Se cierra la ventana de propiedades de vulnerabilidad de software.

La vulnerabilidad de software se ignorará en todos los dispositivos administrados.

*Para ignorar una vulnerabilidad de software en un dispositivo administrado específico:*

1. Abra la ventana de propiedades del dispositivo administrado seleccionado y seleccione la sección **Vulnerabilidades de software**.
2. Seleccione una vulnerabilidad de software.
3. Ignore la vulnerabilidad seleccionada.

La vulnerabilidad de software se ignorará en el dispositivo seleccionado.

Cuando se completen las tareas *Reparar vulnerabilidades* o *Instalar actualizaciones requeridas y reparar vulnerabilidades*, las vulnerabilidades de software ignoradas no se repararán. Las vulnerabilidades ignoradas pueden excluirse de la lista de vulnerabilidades utilizando un filtro.

## Selección de soluciones de usuario para vulnerabilidades de software de terceros

Para usar la tarea *Reparar vulnerabilidades*, debe especificar manualmente las actualizaciones de software para reparar las vulnerabilidades en el software de terceros que se detalla en la configuración de la tarea. La tarea *Reparar vulnerabilidades* utiliza reparaciones recomendadas para el software de Microsoft y reparaciones de usuario para otro software de terceros. Las *correcciones de usuario* son actualizaciones de software para reparar vulnerabilidades que el administrador especifica manualmente para la instalación.

*Para seleccionar reparaciones de usuario para vulnerabilidades en software de terceros, realice lo siguiente:*

1. En la carpeta **Avanzado → Administración de aplicaciones** del árbol de la consola, seleccione la subcarpeta **Vulnerabilidades de software**.

   El espacio de trabajo de la carpeta muestra una lista de las vulnerabilidades que detecta el Agente de red en aplicaciones instaladas en dispositivos.
2. Seleccione la vulnerabilidad para la que desea agregar una solución de usuario.
3. Seleccione **Propiedades** en el menú contextual de la vulnerabilidad.

   Se abre la ventana de propiedades de la vulnerabilidad.
4. En la sección **Correcciones del usuario y otras correcciones**, haga clic en el botón **Agregar**.

   Se muestra una lista de paquetes de instalación disponibles. La lista de paquetes de instalación que se muestran corresponde a la lista **Instalación remota → Paquetes de instalación**. Si no ha creado un paquete de instalación que contenga la reparación del usuario para la vulnerabilidad seleccionada, ahora puede crear el paquete iniciando el Asistente de nuevo paquete.
5. Seleccione uno o más paquetes de instalación que contengan una o más reparaciones del usuario para la vulnerabilidad en el software de terceros.
6. Haga clic en **Aceptar**.

Como resultado, quedan especificados los paquetes de instalación que contengan correcciones de usuario para la vulnerabilidad de software. Cuando se inicie la tarea *Reparar vulnerabilidades*, se instalará el paquete de instalación y se reparará la vulnerabilidad de software.

# Reglas para la instalación de actualizaciones

Para reparar vulnerabilidades en sus aplicaciones, debe definir reglas de instalación de actualizaciones. Estas reglas determinan qué actualizaciones se deben instalar y qué vulnerabilidades se deben reparar.

La configuración exacta de la regla depende de si se la usará con actualizaciones para aplicaciones de Microsoft, con actualizaciones publicadas para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky y Microsoft) o con actualizaciones para cualquier aplicación. Cuando cree una regla para aplicaciones de Microsoft o para aplicaciones de terceros, podrá seleccionar las aplicaciones específicas (y las versiones puntuales de esas aplicaciones) para las que quiera instalar actualizaciones. Cuando cree una regla para cualquier aplicación, podrá seleccionar las actualizaciones específicas que quiera instalar y las vulnerabilidades puntuales que quiera reparar mediante la instalación de actualizaciones.

*Para crear una nueva regla para las actualizaciones de cualquier aplicación:*

1. En la página **Configuración** del Asistente para crear nueva tarea, haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Siga los pasos del asistente.

2. En la página **Tipo de regla**, seleccione **Regla para todas las actualizaciones**.

3. En la página **Criterios generales**, use las listas desplegables para definir los siguientes ajustes:

   - Conjunto de actualizaciones para instalar

     Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

     - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

   - Reparar vulnerabilidades que tengan o superen este nivel de gravedad

     Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

     Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

     Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

     Esta opción está deshabilitada de forma predeterminada.

4. En la página **Actualizaciones**, seleccione las actualizaciones que se instalarán:

   - **Instalar todas las actualizaciones adecuadas**

     Se instalarán todas las actualizaciones de software que cumplan con los criterios especificados en la página **Criterios generales** del asistente. Esta es la opción seleccionada por defecto.

   - **Instalar solo las actualizaciones de la lista**

     Se instalarán únicamente las actualizaciones de software que seleccione manualmente en la lista. La lista contiene todas las actualizaciones de software disponibles.

     Existen situaciones en las que querrá elegir manualmente las actualizaciones que se instalarán: podría suceder, por ejemplo, que quiera evaluar ciertas actualizaciones en un entorno de prueba, que quiera actualizar solo las aplicaciones que considere importantes o que necesite actualizar solo algunas aplicaciones puntuales.

     - **Instalar automáticamente todas las actualizaciones de aplicaciones previas requeridas para instalar las actualizaciones seleccionadas**

       Mantenga habilitada esta opción si está de acuerdo en que, para instalar las actualizaciones seleccionadas, se instalen versiones intermedias de las aplicaciones.

       Si deshabilita esta opción, se instalarán únicamente las versiones de las aplicaciones que haya seleccionado. Deshabilite esta opción si quiere que las aplicaciones se actualicen en forma directa, sin que se trate de instalar versiones intermedias. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

       A modo de ejemplo, imagine que un dispositivo tiene instalada la versión 3 de una aplicación. Quiere actualizar esa versión a la 5, pero la versión 5 solo se puede instalar sobre la versión 4. Si esta opción está habilitada, el software instalará primero la versión 4 y luego la versión 5. Si esta opción está deshabilitada, el software no podrá actualizar la aplicación.

       Esta opción está activada de forma predeterminada.

5. En la página **Vulnerabilidades**, seleccione las vulnerabilidades que se repararán al instalar las actualizaciones seleccionadas:

   - **Reparar todas las vulnerabilidades que coincidan con otros criterios**

     Se repararán todas las vulnerabilidades que cumplan con los criterios especificados en la página **Criterios generales** del asistente. Esta es la opción seleccionada por defecto.

   - **Reparar solo las vulnerabilidades de la lista**

     Se repararán únicamente las vulnerabilidades que seleccione manualmente en la lista. La lista contiene todas las vulnerabilidades detectadas.

     Existen situaciones en las que querrá elegir manualmente las vulnerabilidades que se repararán: podría suceder, por ejemplo, que quiera verificar en un entorno de prueba que las vulnerabilidades se puedan reparar, que quiera reparar las vulnerabilidades solo en las aplicaciones que considere importantes o que prefiera reparar las vulnerabilidades solo en ciertas aplicaciones puntuales.

6. En la página **Nombre**, escriba un nombre para la regla que está creando. Podrá cambiar este nombre más tarde, en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Cuando el Asistente de creación de reglas complete su operación, se creará la nueva regla en el campo **Elija las reglas de instalación de actualizaciones** del Asistente para crear nueva tarea.

*Para crear una nueva regla para las actualizaciones de las aplicaciones de Microsoft:*

1. En la página **Configuración** del Asistente para crear nueva tarea, haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Siga los pasos del asistente.

2. En la página **Tipo de regla**, seleccione **Regla para Windows Update**.

3. En la página **Criterios generales**, defina los siguientes ajustes:

- Conjunto de actualizaciones para instalar

  Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

  - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
  - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
  - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

- Reparar vulnerabilidades que tengan o superen este nivel de gravedad

  Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

  Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

  Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

  Esta opción está deshabilitada de forma predeterminada.

- Reparar vulnerabilidades con un nivel de gravedad de MSRC igual o mayor que

  Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

  Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que el Centro de respuestas de seguridad de Microsoft (MSRC) haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

  Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

  Esta opción está deshabilitada de forma predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desee instalar actualizaciones. Por defecto, están seleccionadas todas las aplicaciones.

5. En la página **Categorías de actualizaciones**, seleccione las actualizaciones para instalar. Las categorías son las mismas que se usan en el Catálogo de Microsoft Update. Por defecto, están seleccionadas todas las categorías.

6. En la página **Nombre**, escriba un nombre para la regla que está creando. Podrá cambiar este nombre más tarde, en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Cuando el Asistente de creación de reglas complete su operación, se creará la nueva regla en el campo **Elija las reglas de instalación de actualizaciones** del Asistente para crear nueva tarea.

*Para crear una nueva regla para las actualizaciones de aplicaciones de terceros:*

1. En la página **Configuración** del Asistente para crear nueva tarea, haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Siga los pasos del asistente.

2. En la página **Tipo de regla**, seleccione **Regla para las actualizaciones de terceros**.

3. En la página **Criterios generales**, defina los siguientes ajustes:

   - Conjunto de actualizaciones para instalar

     Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

     - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

   - Reparar vulnerabilidades que tengan o superen este nivel de gravedad

     Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

     Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

     Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

     Esta opción está deshabilitada de forma predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desea instalar actualizaciones. Por defecto, están seleccionadas todas las aplicaciones.

5. En la página **Nombre**, escriba un nombre para la regla que está creando. Podrá cambiar este nombre más tarde, en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Cuando el Asistente de creación de reglas complete su operación, se creará la nueva regla en el campo **Elija las reglas de instalación de actualizaciones** del Asistente para crear nueva tarea.

# Grupos de aplicaciones

Esta sección describe cómo administrar grupos de aplicaciones instaladas en los dispositivos.

## Creación de categorías de aplicaciones

Kaspersky Security Center permite la creación de categorías de aplicaciones instaladas en dispositivos.

Las categorías de aplicaciones se pueden crear de una de estas formas:

- El administrador especifica una carpeta en la que se han incluido los archivos ejecutables de la categoría seleccionada.
- El administrador especifica un dispositivo a partir del cual los archivos ejecutables deberán incluirse dentro de la categoría seleccionada.
- El administrador establece los criterios que deben usarse para incluir las aplicaciones dentro de la categoría seleccionada.

Cuando se crea la categoría de aplicaciones, el administrador puede establecer reglas para esa categoría. Las reglas definen el comportamiento de las aplicaciones pertenecientes a la categoría especificada. Por ejemplo, puede bloquear o permitir el inicio de las aplicaciones incluidas en la categoría.

## Administrar aplicaciones que se ejecutan en dispositivos

Kaspersky Security Center le permite administrar el inicio de aplicaciones en dispositivos en el modo Lista de admitidos. Para obtener una descripción detallada, consulte la Ayuda en línea de Kaspersky Endpoint Security para Windows. Mientras está activado el modo Lista de admitidos, en los dispositivos seleccionados solo puede iniciar las aplicaciones pertenecientes a las categorías especificadas. El administrador puede visualizar los resultados del análisis estadístico que se ha aplicado a las reglas de inicio de aplicaciones en dispositivos para cada usuario.

## Inventariado del software instalado en los dispositivos

Kaspersky Security Center permite realizar un inventario del software en dispositivos que ejecutan Windows y Linux. El Agente de red recupera información acerca de todas las aplicaciones instaladas en dispositivos. La información recopilada durante el inventario se muestra en el espacio de trabajo de la carpeta **Registro de aplicaciones**. El administrador puede ver información detallada acerca de cualquier aplicación, incluso su versión y el fabricante.

Kaspersky Security Center puede recibir un máximo de 150 000 archivos ejecutables de cada dispositivo cliente. Habiendo alcanzado este límite, Kaspersky Security Center no puede recibir ningún archivo nuevo.

### Administración del grupo de aplicaciones con licencia

Kaspersky Security Center permite crear grupos de aplicaciones con licencia. Un grupo de aplicaciones con licencia incluye aplicaciones que cumplen con los criterios establecidos por el administrador. El administrador puede especificar los criterios siguientes para grupos de aplicaciones con licencia:

- Nombre de la aplicación
- Versión de la aplicación
- Fabricante
- Etiqueta de aplicación

Las aplicaciones que cumplen con uno o varios de los criterios se incluyen automáticamente en un grupo. Para crear un grupo de aplicaciones con licencia, debe establecer por lo menos un criterio de inclusión de aplicaciones en este grupo.

Cada grupo de aplicaciones con licencia dispone de una clave de licencia propia. La clave de licencia de un grupo de aplicaciones con licencia define el número máximo de instalaciones permitidas para las aplicaciones incluidas en ese grupo. Si el número de instalaciones supera el límite que establece la clave de licencia, se registra un evento de información en el Servidor de administración. El administrador puede especificar una fecha de caducidad para la clave de licencia. Cuando llega la fecha, un evento de información se registra en el Servidor de administración.

### Visualización de información sobre archivos ejecutables

Kaspersky Security Center recopila toda la información acerca de los archivos ejecutables que se han ejecutado en dispositivos desde que se instalaron los sistemas operativos en ellos. La información sobre los archivos ejecutables se muestra en la ventana principal de la aplicación, en el espacio de trabajo de la carpeta **Archivos ejecutables**.

## Uso de Control de aplicaciones para administrar archivos ejecutables

Puede utilizar el componente Control de aplicaciones para permitir o bloquear el inicio de archivos ejecutables en los dispositivos del usuario. El componente Control de aplicaciones es compatible con sistemas operativos Windows y Linux.

Para los sistemas operativos Linux, el componente Control de aplicaciones está disponible a partir de Kaspersky Endpoint Security 11.2 para Linux. El componente también está disponible para Kaspersky Embedded Systems Security para Windows 3.0 o posterior.

### Requisitos previos

- Kaspersky Security Center está desplegado en su organización.
- Se ha creado y activado una directiva para Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security para Windows.
- La directiva de Kaspersky Embedded Systems Security for Windows o Kaspersky Embedded Systems Security for Linux ahora está creada y activa.

## Etapas

El procedimiento de uso de Control de aplicaciones consta de etapas:

1. **Crear y ver la lista de archivos ejecutables almacenados en los dispositivos cliente**

   En esta etapa, podrá descubrir qué archivos ejecutables se encuentran guardados en los dispositivos administrados. Revise la lista de archivos ejecutables y compárela con las listas de archivos ejecutables permitidos y prohibidos. Las restricciones sobre el uso de archivos ejecutables pueden estar vinculadas a las políticas de seguridad de la información de su organización.

   Instrucciones:

   - Consola de administración: inventario de archivos ejecutables
   - Kaspersky Security Center Web Console: obtención y visualización de una lista de archivos ejecutables almacenados en los dispositivos cliente

2. **Creación de categorías para archivos ejecutables utilizados en la organización**

   Analice las listas de aplicaciones y archivos ejecutables almacenados en los dispositivos administrados. Cree las categorías para archivos ejecutables en función del análisis. Recomendamos crear una categoría llamada "Aplicaciones de trabajo" que cubra los archivos ejecutables estándar que se utilicen en la organización. Luego, si tiene grupos de seguridad diferentes que trabajan con sus propios archivos ejecutables, puede crear una categoría independiente para cada grupo de seguridad.

   Instrucciones:

   - Consola de administración: Creación de una categoría de aplicaciones con contenido agregado manualmente, Creación de una categoría de aplicaciones que incluya archivos ejecutables de dispositivos seleccionados, Creación de una categoría de aplicaciones que incluya archivos ejecutables de una carpeta específica.
   - Kaspersky Security Center Web Console: Creación de una categoría de aplicaciones con contenido agregado manualmente, Creación de una categoría de aplicaciones que incluya archivos ejecutables de dispositivos seleccionados, Creación de una categoría de aplicaciones que incluya archivos ejecutables de una carpeta seleccionada.

3. **Configurar Control de aplicaciones en la directiva de Kaspersky Endpoint Security**

   Configure el componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security utilizando las categorías que creó en la etapa anterior.

   Instrucciones:

   - Consola de administración: Configuración de la administración de inicio de aplicaciones en dispositivos cliente
   - Kaspersky Security Center Web Console: Configuración del Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows

4. **Configurar el Control de aplicaciones en la directiva de aplicaciones de Kaspersky Embedded Systems Security**

   Configure el componente Control de aplicaciones en la directiva de Kaspersky Embedded Systems Security para Windows utilizando las categorías que ha creado. Para obtener más información sobre el componente Control de aplicaciones, consulte la Ayuda de Kaspersky Embedded Systems Security para Windows o la Ayuda de Kaspersky Embedded Systems Security para Linux.

   Si utiliza una gran cantidad de reglas, puede producirse un error al cargar la directiva. Puede aumentar el tamaño máximo de solicitud en bytes utilizando los siguientes comandos:

- Para la solicitud JSON:

  ```
  klscflag -fset -pv ".core/.independent" -s KLLIM -n
  LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v <max_request_size> -t d
  ```

- Para la solicitud HTTP:

  ```
  klscflag -fset -pv ".core/.independent" -s KLLIM -n
  LP_KLOAPI_MaxSizeOfHttpRequestInBytes -v <max_request_size> -t d
  ```

  Dónde `<max_request_size>` es el tamaño máximo de solicitud en bytes (por ejemplo, `200000000`).

5. **Activar el componente Control de aplicaciones en modo de prueba**

   Las reglas de Control de aplicaciones no deben bloquear los archivos ejecutables que los usuarios necesiten para trabajar. Para asegurarse de que esto sea así, cuando cree nuevas reglas de Control de aplicaciones, recomendamos que habilite un modo de prueba y analice el funcionamiento de las reglas. Mientras estas pruebas se encuentren activas, Kaspersky Endpoint Security para Windows o Kaspersky Embedded Systems Security no bloqueará los archivos ejecutables que las reglas de Control de aplicaciones no permitan iniciar, sino que simplemente notificará al Servidor de administración para informar de que tales aplicaciones se han iniciado.

   Para probar las reglas de Control de aplicaciones, recomendamos que haga lo siguiente:

   - Defina la duración del período de prueba. El período de prueba puede durar de varios días a dos meses.
   - Examine los eventos que surjan de probar el funcionamiento de Control de aplicaciones.

   Instrucciones para Kaspersky Security Center Web Console: Configuración del componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows. Siga estas instrucciones y habilite la opción **Modo de prueba** en el proceso de configuración.

6. **Cambiar la configuración de las categorías en el componente Control de aplicaciones**

   De ser necesario, modifique la configuración de Control de aplicaciones. Con los resultados de las pruebas, puede crear una categoría con contenido agregado manualmente que incluya los archivos ejecutables vinculados a los eventos de Control de aplicaciones.

   Instrucciones:

   - Consola de administración: Adición de archivos ejecutables relacionados con un evento a una categoría de aplicaciones
   - Kaspersky Security Center Web Console: Adición de archivos ejecutables relacionados con un evento a una categoría de aplicaciones

7. **Aplicar las reglas de Control de aplicaciones en modo de funcionamiento normal**

   Después de probar las reglas de Control de aplicaciones y completar la configuración de las categorías, podrá aplicar las reglas de Control de aplicaciones en el modo de operación.

   Instrucciones para Kaspersky Security Center Web Console: Configuración del componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows. Siga estas instrucciones y deshabilite la opción **Modo de prueba** en el proceso de configuración.

8. **Verificar la configuración de Control de aplicaciones**

   Asegúrese de haber hecho lo siguiente:

   - Categorías de archivos ejecutables creadas.
   - Configuración de Control de aplicaciones con las categorías.
   - Aplicar las reglas de Control de aplicaciones en el modo de operación.

### Resultados

Al concluir este procedimiento, el inicio de archivos ejecutables en los dispositivos administrados estará bajo su control. Los usuarios pueden iniciar solo aquellos archivos ejecutables que están permitidos en su organización y no pueden iniciar los que están prohibidos.

Para obtener información detallada sobre el Control de aplicaciones, consulte los siguientes temas de ayuda:

- Ayuda en línea de Kaspersky Endpoint Security para Windows
- Ayuda en línea de Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Ayuda de Kaspersky Embedded Systems Security para Windows
- Ayuda de Kaspersky Embedded Systems Security para Linux

## Obtención y visualización de una lista de archivos ejecutables almacenados en los dispositivos cliente

Puede obtener la lista de archivos ejecutables almacenados en los dispositivos cliente de una de las siguientes maneras:

- Habilitando las notificaciones sobre el inicio de aplicaciones en la directiva de Kaspersky Endpoint Security.
- Creando una tarea de inventario.

### Habilitando las notificaciones sobre el inicio de aplicaciones en la directiva de Kaspersky Endpoint Security

*Para habilitar las notificaciones sobre la ejecución de aplicaciones:*

1. Abra la configuración de la directiva de Kaspersky Endpoint Security y luego vaya a **Configuración general** → **Informes y almacenamiento**.
2. En el grupo de configuración **Transferencia de datos al servidor de administración**, seleccione la casilla de verificación **Acerca de las aplicaciones iniciadas** y guarde los cambios.

Cuando un usuario intenta iniciar archivos ejecutables, la información sobre estos archivos se añade a la lista de archivos ejecutables en el dispositivo cliente. Kaspersky Endpoint Security envía esta información al Agente de red, que a su vez la envía al Servidor de administración.

## Crear una tarea de inventario

La función de inventario de archivos ejecutables está disponible para las siguientes aplicaciones:

- Kaspersky Endpoint Security para Windows
- Kaspersky Endpoint Security for Linux (versión 11.2 y posteriores)
- Kaspersky Security for Virtualization 4.0 Light Agent y versiones posteriores

Puede reducir la carga a la que se somete la base de datos cuando se obtiene información sobre las aplicaciones instaladas. Para ahorrar espacio, recomendamos que ejecute una tarea de inventario en los dispositivos de referencia que tengan instalada una selección de aplicaciones estándar. El número preferible de dispositivos es de 1 a 3.

Desaconsejamos ejecutar la tarea de inventario si se utilizan las siguientes bases de datos: MySQL, PostgreSQL, SQL Server Express Edition, MariaDB (cualquier edición).

*Para crear una tarea que haga un inventario de los archivos ejecutables instalados en los dispositivos cliente:*

1. En el árbol de la consola, seleccione la carpeta **Tareas**.
2. En el espacio de trabajo de la carpeta **Tareas**, haga clic en el botón **Nueva tarea**.

   Se inicia el Asistente para crear nueva tarea.
3. En la ventana **Seleccione el tipo de tarea** del asistente, seleccione **Kaspersky Endpoint Security** como el tipo de tarea; a continuación, seleccione **Inventario** como subtipo de tarea y haga clic en **Siguiente**.
4. Siga el resto de instrucciones del asistente.

   Una vez que finalice el Asistente para crear nueva tarea, se creará y configurará la tarea **Inventario**. Si lo desea, puede cambiar la configuración de la tarea creada. Encontrará la nueva tarea en la lista de tareas. Si lo desea, puede cambiar la configuración de la tarea creada.

Para obtener una descripción detallada de la tarea de inventario, consulte las siguientes ayudas:

- Ayuda de Kaspersky Endpoint Security para Windows
- Ayuda de Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Una vez efectuada la tarea **Inventario**, se crea la lista de archivos ejecutables almacenados en los dispositivos administrados para que pueda verla.

Durante el inventario, se pueden detectar archivos ejecutables en los siguientes formatos (dependiendo de la opción que seleccione en las propiedades de la tarea de inventario): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR y HTML.

### Consultar las listas de archivos ejecutables almacenados en los dispositivos administrados

*Para visualizar la lista de los archivos ejecutables almacenados en los dispositivos cliente, haga lo siguiente:*

En el árbol de la consola, vaya a **Avanzado** → **Administración de aplicaciones** → **Archivos ejecutables**.

Si es necesario, puede enviar un archivo ejecutable desde un dispositivo administrado al dispositivo que tenga instalada la Consola de administración.

*Para enviar un archivo ejecutable:*

1. En el árbol de la consola, vaya a **Avanzado** → **Administración de aplicaciones** → **Archivos ejecutables**.
2. Haga clic en el vínculo del archivo ejecutable que desea enviar al dispositivo que tenga instalada la Consola de administración.
3. En la ventana que se abre, vaya a **Dispositivos** y seleccione la casilla del dispositivo administrado desde el que desea enviar el archivo ejecutable.

   Antes de enviar el archivo ejecutable, asegúrese de que el dispositivo administrado tiene una conexión directa con el Servidor de administración, seleccionando la casilla de verificación **No desconectar del Servidor de administración**.

4. Haga clic en el botón **Enviar**, seleccione la carpeta de destino y luego haga clic en **Aceptar**.

   El archivo ejecutable seleccionado se descarga para su posterior envío al dispositivo que tenga instalada la Consola de administración.

## Creación de categorías de aplicaciones para las directivas de Kaspersky Endpoint Security para Windows

Puede crear categorías de aplicaciones para las directivas de Kaspersky Endpoint Security para Windows desde la carpeta **Categorías de aplicaciones** y desde la ventana **Propiedades** de una directiva de Kaspersky Endpoint Security para Windows.

*Para crear una categoría de aplicación para una directiva de Kaspersky Endpoint Security desde la carpeta de **Categorías de aplicaciones**:*

1. En el árbol de la consola, seleccione **Avanzado** → **Administración de aplicaciones** → **Categorías de aplicaciones**.
2. En el espacio de trabajo de la carpeta **Categorías de aplicaciones**, haga clic en el botón **Nueva categoría**.

   Se inicia el Asistente para crear nueva categoría.

3. En la página **Tipo de categoría**, seleccione el tipo de categoría de usuario:

   - **Categorías con contenido agregado de forma manual**. Especifique los criterios que serán usados para asignar archivos ejecutables a la categoría creada.
   - **Categoría con contenido agregado de forma automática**. Especifique la carpeta desde la cual los archivos ejecutables automáticamente se asignarán a la categoría creada.

     Al crear una categoría con contenido que se agrega automáticamente, la aplicación realiza el inventario de los siguientes tipos de archivo: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX y SCR.

   - **Categoría que incluye los archivos ejecutables de los dispositivos seleccionados**. Especifique un dispositivo cuyos archivos ejecutables automáticamente se asignarán a la categoría.

4. Siga las instrucciones del asistente.

   Cuando el Asistente finaliza, se crea una categoría de aplicación personalizada. Se pueden ver las categorías creadas recientemente mediante la lista de categorías del espacio de trabajo de la carpeta **Categorías de aplicaciones**.

Si desea exportar una categoría de aplicación a un archivo KLC, haga clic derecho en el nombre de la categoría, seleccione **Exportar** en el menú y luego, en la ventana que aparece, indique el nombre del archivo y haga clic en **Guardar**.

También puede crear una categoría de aplicación desde la carpeta **Directivas**.

*Para crear una categoría de aplicación desde la ventana **Propiedades** de una directiva de Kaspersky Endpoint Security para Windows:*

1. En el árbol de la consola, seleccione la carpeta **Directivas**.
2. En el espacio de trabajo de la carpeta **Directivas**, seleccione una directiva de Kaspersky Endpoint Security para la cual desea crear una categoría.
3. Haga clic derecho y seleccione **Propiedades**.
4. En la ventana **Propiedades** que se abre, en el panel **Secciones** de la izquierda, seleccione **Controles de seguridad → Control de aplicaciones**.
5. En la sección **Control de aplicaciones**, en el **Modo de control** y en las listas desplegables de **Acción**, realice las selecciones para la lista de admitidos o la lista de rechazados, y luego haga clic en el botón **Agregar**.

   Se abrirá la ventana **Regla de Control de aplicaciones**, que contendrá una lista de categorías.
6. Haga clic en el botón **Crear nueva**.
7. Ingrese el nombre de la nueva categoría y haga clic en **Aceptar**.

   Se inicia el Asistente para crear nueva categoría.

8. En la página **Tipo de categoría**, seleccione el tipo de categoría de usuario:

   - **Categorías con contenido agregado de forma manual**. Especifique los criterios que serán usados para asignar archivos ejecutables a la categoría creada.
   - **Categoría con contenido agregado de forma automática**. Especifique la carpeta desde la cual los archivos ejecutables automáticamente se asignarán a la categoría creada.

     Al crear una categoría con contenido que se agrega automáticamente, la aplicación realiza el inventario de los siguientes tipos de archivo: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX y SCR.

   - **Categoría que incluye los archivos ejecutables de los dispositivos seleccionados**. Especifique un dispositivo cuyos archivos ejecutables automáticamente se asignarán a la categoría.

9. Siga las instrucciones del asistente.

Cuando el Asistente finaliza, se crea una categoría de aplicación personalizada. Puede ver las categorías recién creadas en la lista de categorías.

El componente Control de aplicaciones incluido en Kaspersky Endpoint Security para Windows utiliza las categorías de aplicaciones. El Control de aplicaciones permite que el administrador imponga restricciones al inicio de aplicaciones en dispositivos cliente, por ejemplo, restringiendo los inicios a aplicaciones en una categoría especificada.

## Creación de una categoría de aplicaciones con contenido agregado manualmente

Puede especificar un conjunto de criterios que sean comunes a los archivos ejecutables que los usuarios podrán o no podrán iniciar en su organización. Puede agregar los archivos que respondan a estos criterios a una nueva categoría de aplicaciones. Más tarde, podrá usar esa nueva categoría para configurar el componente Control de aplicaciones.

*Para crear una categoría de aplicaciones con contenido agregado manualmente:*

1. En el árbol de consola, en la carpeta **Avanzado** → **Administración de aplicaciones**, seleccione la subcarpeta **Categorías de aplicaciones**.
2. Haga clic en el botón **Nueva categoría**.

   Se inicia el **Asistente para crear nueva categoría**. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
3. En la página **Tipo de categoría** del Asistente, selección **Categoría con contenido agregado manualmente** como el tipo de categoría de usuario.
4. En la página del asistente **Escriba el nombre de la categoría de aplicaciones**, ingrese el nuevo nombre de categoría de la aplicación.
5. En la página **Configure las condiciones que se usarán para incluir aplicaciones en las categorías**, haga clic en el botón **Agregar**.

6. En la lista desplegable, especifique la configuración correspondiente:

- **De la lista de archivos ejecutables**

  Seleccione esta opción si desea elegir las aplicaciones que se agregarán a la categoría de la lista de archivos ejecutables almacenados en el dispositivo cliente.

- **De las propiedades de archivo**

  Si se selecciona esta opción, puede especificar los datos detallados de los archivos ejecutables que se agregarán a la categoría de aplicaciones del usuario.

- **Metadatos de los archivos de la carpeta**

  Especifique una carpeta en el dispositivo cliente que contenga archivos ejecutables. Los metadatos de los archivos ejecutables que están incluidos en la carpeta especificada se enviarán al Servidor de administración. Los archivos ejecutables que contienen los mismos metadatos se agregarán a la categoría de aplicaciones del usuario.

- **Sumas de comprobación de los archivos de la carpeta**

  Si se selecciona esta opción, puede seleccionar o crear una carpeta en el dispositivo cliente. El hash MD5 de los archivos en la carpeta especificada se enviará al Servidor de administración. Las aplicaciones que tienen los mismos hash que los archivos en la carpeta especificada, se agregan a la categoría de aplicaciones del usuario.

- **Certificados de los archivos de la carpeta**

  Si se selecciona esta opción, puede especificar la carpeta en el dispositivo cliente que contenga archivos ejecutables firmados con certificados. Los certificados de archivos ejecutables se leen y se agregan a las condiciones de la categoría. Los archivos ejecutables que se hayan firmado conforme a esos certificados se agregarán a la categoría personalizada.

- **Metadatos de los archivos del instalador MSI**

  Seleccione esta opción para especificar un archivo de instalador MSI como condición para agregar aplicaciones a la categoría personalizada. Los metadatos del instalador se enviarán al Servidor de administración. Las aplicaciones que tengan los mismos metadatos de instalador que el instalador MSI especificado se agregarán a la categoría de aplicaciones personalizada.

- **Sumas de comprobación de los archivos incluidos en el instalador MSI de la aplicación**

  Seleccione esta opción para especificar un archivo de instalador MSI como condición para agregar aplicaciones a la categoría personalizada. El hash de los archivos del instalador de la aplicación se enviará al Servidor de administración. Las aplicaciones para las cuales el hash de archivos del instalador MSI es idéntico al hash especificado se agregan a la categoría de aplicaciones del usuario.

- **De la categoría KL**

Seleccione esta opción si, como condición para agregar aplicaciones a la categoría personalizada, desea elegir una categoría de aplicaciones de Kaspersky. Las aplicaciones que pertenezcan a la categoría de Kaspersky elegida se agregarán a la categoría de aplicaciones personalizada.

- **Especificar la ruta a la aplicación (se pueden usar máscaras)**

  Seleccione esta opción para especificar la ruta a un archivo o carpeta del dispositivo cliente que contenga los archivos ejecutables que quiera agregar a la categoría de aplicaciones personalizada. Puede utilizar expresiones regulares como *C:\path_to_exe**, por ejemplo: *C:\Program Files\Internet Explorer**.

- **Seleccionar el certificado del repositorio**

  Seleccione esta opción para elegir certificados almacenados en el repositorio. La condición de la categoría solo coincide con los archivos ejecutables que están firmados por el certificado especificado.

  Los certificados se agregan al repositorio si creó e inició una tarea de inventario o marcó la casilla **Acerca de las aplicaciones iniciadas** en la directiva de Kaspersky Endpoint Security. Puede realizar ambas acciones.

- **Tipo de unidad**

  Seleccione esta opción para especificar el tipo de soporte (unidad extraíble o cualquier tipo de unidad) desde el que se ejecuta la aplicación. Las aplicaciones que se inicien desde el tipo de unidad seleccionado se agregarán a la categoría de aplicaciones personalizada.

7. En la página del asistente **Crear la categoría de aplicaciones**, haga clic en el botón **Finalizar**.

Kaspersky Security Center solo gestiona metadatos de archivos firmados digitalmente. No se puede crear ninguna categoría sobre la base de metadatos de archivos que no contengan una firma digital.

Cuando el Asistente finaliza, se crea una categoría de aplicaciones del usuario con contenido agregado manualmente. Puede ver la categoría recién creada utilizando la lista de categorías en el espacio de trabajo de la carpeta **Categorías de aplicaciones**.

Si desea exportar una categoría de aplicación a un archivo KLC, haga clic derecho en el nombre de la categoría, seleccione **Exportar** en el menú y luego, en la ventana que aparece, indique el nombre del archivo y haga clic en **Guardar**.

## Crear una categoría de aplicaciones con archivos ejecutables de dispositivos específicos

Puede usar archivos ejecutables almacenados en ciertos dispositivos puntuales como modelo de los archivos ejecutables que quiera permitir o bloquear. Los archivos ejecutables de estos dispositivos pueden servirle de base para crear una categoría de aplicaciones, que luego podrá usar en la configuración del componente Control de aplicaciones.

*Para recuperar la lista de archivos ejecutables de los dispositivos:*

1. Asegúrese de que creó y activó una directiva para Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security para Windows. Habilite el componente Control de aplicaciones en la directiva.

2. Obtenga una lista de archivos ejecutables almacenados en los dispositivos cliente.

*Para crear una categoría de aplicaciones que incluya archivos ejecutables de dispositivos seleccionados:*

1. En el árbol de consola, en la carpeta **Avanzado** → **Administración de aplicaciones**, seleccione la subcarpeta **Categorías de aplicaciones**.

2. Haga clic en el botón **Nueva categoría**.

   Se inicia el **Asistente para crear nueva categoría**. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. En la página del asistente **Tipo de categoría**, seleccione **Categoría que incluye archivos ejecutables de dispositivos seleccionados** como tipo de categoría de usuario.

4. En la página del asistente **Escriba el nombre de la categoría de aplicaciones**, ingrese el nuevo nombre de categoría de la aplicación.

5. En la página del asistente **Configuración**, haga clic en el botón **Agregar**.

6. Seleccione un dispositivo o los dispositivos cuyos archivos ejecutables se utilizarán para crear la categoría de aplicaciones.

7. Configure los siguientes ajustes:

- **Algoritmo de evaluación del valor de hash**

  Según la versión de la aplicación de seguridad instalada en los dispositivos en su red, debe seleccionar un algoritmo para que Kaspersky Security Center calcule el valor de hash para archivos en esta categoría. La información sobre los valores hash calculados por las funciones hash se almacena en la base de datos del Servidor de administración.

  SHA256 es una función de hash criptográfica. En la actualidad, se la considera la más confiable en su clase, pues no se encontró vulnerabilidad alguna en su algoritmo. Kaspersky Endpoint Security puede calcular hashes SHA256 desde la versión 10 Service Pack 2 para Windows. Las versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows son compatibles con la función de hash MD5.

  Seleccione cualquiera de las opciones de evaluación del valor de hash de Kaspersky Security Center para archivos en la categoría:

  - Si todas las instancias de aplicaciones de seguridad instaladas en su red son Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores, marque la casilla **SHA256**. Si hay versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows en su red, recomendamos que no agregue categorías que utilicen como criterio el hash SHA256 del archivo ejecutable. Si lo hace, la aplicación de seguridad podría no funcionar correctamente. De presentarse inconvenientes, utilice la función de hash criptográfico MD5 para los archivos de la categoría.

  - Si hay alguna versión anterior a Kaspersky Endpoint Security 10 Service Pack 2 para Windows instalada en su red, seleccione **Hash MD5**. No puede agregar una categoría que se haya creado según el criterio de la suma de verificación MD5 de un archivo ejecutable para Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores. De presentarse inconvenientes, utilice la función de hash criptográfico SHA256 para los archivos de la categoría.

  Si diferentes dispositivos en su red usan versiones anteriores y posteriores de Kaspersky Endpoint Security 10, marque la casilla **SHA256** y la casilla **Hash MD5**.

  La casilla **Calcular SHA256 para los archivos de esta categoría (compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)** está activada de manera predeterminada.

  De manera predeterminada, la casilla **Calcular MD5 para los archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)** está desactivada.

- **Sincronizar datos con el repositorio del Servidor de administración**

  Seleccione esta opción si desea que el Servidor de administración verifique periódicamente si ha habido cambios en la(s) carpeta(s) especificada(s).

  Esta opción está deshabilitada de forma predeterminada.

  Si habilita esta opción, indique la frecuencia (en horas) con la que se llevará a cabo la verificación. Por defecto, se realiza una búsqueda de cambios cada veinticuatro horas.

8. En la página del asistente **Filtro**, especifique la siguiente configuración:

   - Tipo de archivo

     Utilice esta sección para especificar qué clase de archivos se usarán para crear la categoría de aplicaciones.

     **Todos los archivos**. Para crear la categoría, se tendrán en cuenta todos los archivos. Esta opción está seleccionada de forma predeterminada.

     **Solo archivos fuera de las categorías de aplicaciones**. Para crear la categoría, solo se tendrán en cuenta los archivos que no estén incluidos en las categorías de aplicaciones.

   - Carpetas

     Utilice esta sección para elegir las carpetas del dispositivo (o de los dispositivos) que contengan los archivos que se usarán para crear la categoría de aplicaciones.

     **Todas las carpetas**. Para crear la categoría, se tendrán en cuenta todas las carpetas. Esta opción está seleccionada de forma predeterminada.

     **Carpeta especificada**: Para crear la categoría, solo se tendrá en cuenta la carpeta especificada. Si selecciona esta opción, deberá especificar la ruta a la carpeta.

9. En la página del asistente **Crear la categoría de aplicaciones**, haga clic en el botón **Finalizar**.

   Cuando el asistente finaliza, se crea una categoría de aplicación de usuario. Puede ver la categoría recién creada utilizando la lista de categorías en el espacio de trabajo de la carpeta **Categorías de aplicaciones**.

Si desea exportar una categoría de aplicación a un archivo KLC, haga clic derecho en el nombre de la categoría, seleccione **Exportar** en el menú y luego, en la ventana que aparece, indique el nombre del archivo y haga clic en **Guardar**.

## Creación de una categoría de aplicaciones que incluya archivos ejecutables de una carpeta específica

Puede usar archivos ejecutables de una carpeta seleccionada como el estándar de archivos ejecutables que desea permitir o bloquear en su organización. Sobre la base de los archivos ejecutables de la carpeta seleccionada, puede crear una categoría de aplicaciones y usarla en la configuración del componente Control de aplicaciones.

*Para crear una categoría de aplicaciones que incluya archivos ejecutables de la carpeta seleccionada, haga lo siguiente:*

1. En el árbol de consola, en la carpeta **Avanzado** → **Administración de aplicaciones**, seleccione la subcarpeta **Categorías de aplicaciones**.

2. Haga clic en el botón **Nueva categoría**.

   Se inicia el **Asistente para crear nueva categoría**. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. En la página del asistente **Tipo de categoría**, seleccione **Categoría que incluye archivos ejecutables de una carpeta específica** como tipo de categoría de usuario.

4. En la página del asistente **Escriba el nombre de la categoría de aplicaciones**, ingrese el nuevo nombre de categoría de la aplicación.

5. En la página del asistente **Carpeta de repositorio**, haga clic en el botón **Examinar**.

6. Especifique la carpeta con los archivos ejecutables que se utilizarán para crear la categoría de aplicaciones.

7. Defina los siguientes parámetros de configuración:

- Incluir DLL en esta categoría

  La categoría de aplicaciones incluye bibliotecas de enlace dinámico (archivos en el formato de DLL) y el componente Control de aplicaciones registra las acciones de esas bibliotecas que se ejecutan en el sistema. Incluir archivos DLL en la categoría podría reducir el rendimiento de Kaspersky Security Center.

  Esta casilla no está marcada de manera predeterminada.

- Incluir datos de scripts en esta categoría

  La categoría de aplicaciones incluye datos sobre scripts, y los scripts no son bloqueados por el componente Protección contra amenazas web. Incluir los datos del script en la categoría podría reducir el rendimiento de Kaspersky Security Center.

  Esta casilla no está marcada de manera predeterminada.

- Algoritmo de evaluación del valor de hash: **Calcular el hash SHA256 de los archivos de esta categoría (opción compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)/Calcular MD5 para los archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)**

Según la versión de la aplicación de seguridad instalada en los dispositivos en su red, debe seleccionar un algoritmo para que Kaspersky Security Center calcule el valor de hash para archivos en esta categoría. La información sobre los valores hash calculados por las funciones hash se almacena en la base de datos del Servidor de administración.

SHA256 es una función de hash criptográfica. En la actualidad, se la considera la más confiable en su clase, pues no se encontró vulnerabilidad alguna en su algoritmo. Kaspersky Endpoint Security puede calcular hashes SHA256 desde la versión 10 Service Pack 2 para Windows. Las versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows son compatibles con la función de hash MD5.

Seleccione cualquiera de las opciones de evaluación del valor de hash de Kaspersky Security Center para archivos en la categoría:

- Si todas las instancias de aplicaciones de seguridad instaladas en su red son Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores, marque la casilla **SHA256**. Si hay versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows en su red, recomendamos que no agregue categorías que utilicen como criterio el hash SHA256 del archivo ejecutable. Si lo hace, la aplicación de seguridad podría no funcionar correctamente. De presentarse inconvenientes, utilice la función de hash criptográfico MD5 para los archivos de la categoría.

- Si hay alguna versión anterior a Kaspersky Endpoint Security 10 Service Pack 2 para Windows instalada en su red, seleccione **Hash MD5**. No puede agregar una categoría que se haya creado según el criterio de la suma de verificación MD5 de un archivo ejecutable para Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores. De presentarse inconvenientes, utilice la función de hash criptográfico SHA256 para los archivos de la categoría.

Si diferentes dispositivos en su red usan versiones anteriores y posteriores de Kaspersky Endpoint Security 10, marque la casilla **SHA256** y la casilla **Hash MD5**.

La casilla **Calcular SHA256 para los archivos de esta categoría (compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)** está activada de manera predeterminada.

De manera predeterminada, la casilla **Calcular MD5 para los archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)** está desactivada.

- Forzar análisis de cambios en carpeta

Si se habilita esta opción, la aplicación buscará con frecuencia cambios en la carpeta de incorporación de contenido de categorías. Puede especificar la frecuencia de las búsquedas (en horas) en el campo de entrada que se encuentra al lado de la casilla de verificación. De forma predeterminada, el intervalo entre búsquedas forzadas es de 24 horas.

Si se deshabilita esta opción, la aplicación no forzará la búsqueda en la carpeta. El servidor intenta acceder a los archivos si se modificaron, agregaron o eliminaron.

Esta opción está deshabilitada de forma predeterminada.

8. En la página del asistente **Crear la categoría de aplicaciones**, haga clic en el botón **Finalizar**.

Cuando el asistente finaliza, se crea una categoría de aplicación de usuario. Puede ver la categoría recién creada utilizando la lista de categorías en el espacio de trabajo de la carpeta **Categorías de aplicaciones**.

Si desea exportar una categoría de aplicación a un archivo KLC, haga clic derecho en el nombre de la categoría, seleccione **Exportar** en el menú y luego, en la ventana que aparece, indique el nombre del archivo y haga clic en **Guardar**.

# Agregar archivos ejecutables vinculados a eventos a una categoría de aplicaciones

Los archivos ejecutables relacionados con los eventos **Inicio de aplicación prohibido** e **Inicio de aplicación prohibido en el modo de prueba** pueden agregarse a una categoría de aplicaciones nueva o a una categoría de aplicaciones con contenido agregado de forma manual que ya exista.

*Para agregar a una categoría de aplicaciones los archivos ejecutables relacionados con estos eventos de Control de aplicaciones:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la pestaña **Eventos**.
3. En la pestaña **Eventos**, seleccione los eventos requeridos.
4. En el menú contextual de uno de los eventos seleccionados, seleccione **Añadir categoría**.

5. En la ventana **Acción sobre el archivo ejecutable relacionado con el evento** que se abre, configure las opciones pertinentes:

   Seleccione uno de los siguientes:

   - **Agregar a una nueva categoría de aplicación**

     Seleccione esta opción si desea crear una nueva categoría de aplicaciones.

     Haga clic en el botón **OK** para iniciar el Asistente para crear nueva categoría. Cuando el Asistente finaliza, se crea la categoría con la configuración especificada.

     Esta opción no está seleccionada de manera predeterminada.

   - **Agregar a una categoría de aplicación existente**

     Seleccione esta opción si tiene que agregar reglas a una categoría de aplicaciones existente. Seleccione la categoría relevante en la lista de categorías de aplicaciones.

     Esta opción está seleccionada de forma predeterminada.

   En la sección **Tipo de regla**, seleccione uno de los siguientes ajustes de configuración:

   - **Agregar a categoría**

     Seleccione esta opción si tiene que agregar reglas a las condiciones de la categoría de aplicaciones.

     Esta opción está seleccionada de forma predeterminada.

   - **Reglas para añadir a las exclusiones**

     Seleccione esta opción si desea agregar reglas a las exclusiones de la categoría de aplicaciones.

   En la sección **Tipo de información del archivo**, seleccione uno de los siguientes ajustes de configuración:

   - **Detalles del certificado (o de la función hash SHA256 para archivos sin certificado)**

     Los archivos pueden estar firmados con un certificado. Cada certificado puede utilizarse para firmar más de un archivo. Un mismo certificado puede usarse para firmar distintas versiones de una misma aplicación, por ejemplo, o distintas aplicaciones de un mismo proveedor. Cuando seleccione un certificado, podría suceder que la categoría termine con varias versiones de una misma aplicación o con varias aplicaciones de un mismo proveedor.

     Cada archivo tiene su propia función hash SHA256. Si selecciona una función hash SHA256, solo se agregará a la categoría el archivo específico que se corresponda con ese hash (por ejemplo, la versión especificada de la aplicación).

     Seleccione esta opción si desea agregar los detalles del certificado de un archivo ejecutable (o la función hash SHA256 de los archivos sin certificado) a las reglas de la categoría.

     Esta opción está seleccionada de forma predeterminada.

   - **Detalles del certificado (los archivos sin certificado se omitirán)**

Los archivos pueden estar firmados con un certificado. Cada certificado puede utilizarse para firmar más de un archivo. Un mismo certificado puede usarse para firmar distintas versiones de una misma aplicación, por ejemplo, o distintas aplicaciones de un mismo proveedor. Cuando seleccione un certificado, podría suceder que la categoría termine con varias versiones de una misma aplicación o con varias aplicaciones de un mismo proveedor.

Seleccione esta opción si desea agregar los detalles del certificado de un archivo ejecutable a las reglas de la categoría. Si el archivo ejecutable no tiene certificado, el archivo se omitirá. No se agregará información sobre ese archivo a la categoría.

- **Solo SHA256 (los archivos sin hash se omitirán)**

  Cada archivo tiene su propia función hash SHA256. Si selecciona una función hash SHA256, solo se añadirá a la categoría el archivo específico que se corresponda con ese hash (por ejemplo, la versión especificada de la aplicación).

  Seleccione esta opción si solo desea añadir los detalles de la función hash SHA256 del archivo ejecutable.

- **Solo MD5 (modo discontinuado, solo para Kaspersky Endpoint Security 10 Service Pack 1)**

  Cada archivo tiene su propia función hash MD5. Si selecciona una función hash MD5, solo se agregará a la categoría el archivo específico que se corresponda con ese hash (por ejemplo, la versión especificada de la aplicación).

  Seleccione esta opción si solo desea agregar los detalles de la función hash MD5 del archivo ejecutable. La capacidad de calcular hashes MD5 está disponible para Kaspersky Endpoint Security 10 Service Pack 1 para Windows y versiones anteriores.

6. Haga clic en **Aceptar**.

## Configuración de la administración de inicio de aplicaciones en dispositivos cliente

La categorización de aplicaciones le permite optimizar la administración de las aplicaciones que se ejecutan en los dispositivos. Puede crear una categoría de aplicación y configurar el Control de aplicaciones para una directiva, de modo que solo las aplicaciones de la categoría especificada se inicien en dispositivos a los cuales se aplique esa directiva. Por ejemplo, ha creado una categoría que incluye aplicaciones llamadas *Application_1* y *Application_2*. Después de que agrega esta categoría a una directiva, solo dos aplicaciones se pueden iniciar en dispositivos a los cuales esa directiva se aplica: *Application_1* y *Application_2*. Si un usuario intenta iniciar una aplicación que no se ha incluido en esa categoría, por ejemplo, *Application_3*, esta aplicación se bloquea para que no se inicie. Se muestra al usuario una notificación que informa que el inicio de *Application_3* está bloqueado, de acuerdo con una regla de Control de aplicaciones. Puede crear una categoría con el contenido agregado automáticamente según diferentes criterios desde una carpeta específica. En este caso, los archivos automáticamente se agregan a la categoría desde la carpeta especificada. Los archivos ejecutables de las aplicaciones se copian a la carpeta especificada y se procesan automáticamente; su métrica se agrega a la categoría.

*Para configurar la administración de ejecución de aplicaciones en los dispositivos cliente:*

1. En la carpeta **Avanzado → Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Categorías de aplicaciones**.

2. En el espacio de trabajo de la carpeta **Categorías de aplicaciones**, cree la categoría de aplicaciones que desea administrar mientras se inician.

3. En la carpeta **Dispositivos administrados**, en la pestaña **Directivas**, haga clic en el botón **Nueva directiva** para crear una nueva directiva de Kaspersky Endpoint Security para Windows, y siga las instrucciones del asistente.

   Si esa directiva ya existe, puede omitir este paso. Puede configurar la administración de inicio de aplicaciones en una categoría especificada mediante la configuración de esta directiva. La directiva que se creó recientemente aparece en la carpeta **Dispositivos administrados**, en la pestaña **Directivas**.

4. Seleccione **Propiedades** en el menú contextual de la directiva de Kaspersky Endpoint Security para Windows.

   Se abre la ventana de propiedades de la directiva de Kaspersky Endpoint Security para Windows.

5. En la ventana de propiedades de la directiva de Kaspersky Endpoint Security para Windows, en la sección **Controles de seguridad → Control de aplicaciones**, seleccione la casilla de verificación **Control de aplicaciones**.

6. Haga clic en el botón **Agregar**.

   Se abre la ventana **Regla de Control de aplicaciones**.

7. En la ventana de **Regla de Control de aplicaciones**, en la lista desplegable **Categoría**, seleccione la categoría de aplicaciones que abarque la regla de inicio. Configure la regla de inicio para la categoría de aplicaciones seleccionada.

   Para Kaspersky Endpoint Security 10 Service Pack 2 y versiones posteriores, ninguna categoría se muestra si se crearon sobre la base del criterio de hash MD5 de un archivo ejecutable.

   Si hay versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 en su red, recomendamos que no agregue categorías que utilicen como criterio el hash SHA256 del archivo ejecutable. Esto puede causar errores de la aplicación.

   En la Ayuda en línea de Kaspersky Endpoint Security para Windows encontrará instrucciones detalladas sobre la configuración de reglas de control.

8. Haga clic en **Aceptar**.

Las aplicaciones se ejecutarán en dispositivos incluidos en la categoría especificada según la regla que ha creado. La regla creada aparece en la ventana de propiedades de la directiva de Kaspersky Endpoint Security para Windows, en la sección **Control de aplicaciones**.

## Visualización de los resultados del análisis estático de las reglas de inicio aplicadas a los archivos ejecutables

*Para ver información acerca de los archivos ejecutables que los usuarios no están autorizados a ejecutar:*

1. En la carpeta **Dispositivos administrados** del árbol de consola, seleccione la pestaña **Directivas**.

2. Seleccione **Propiedades** en el menú contextual de la directiva de Kaspersky Endpoint Security para Windows.

   Se abre la ventana de propiedades de la directiva de aplicación.

3. En el recuadro **Secciones**, seleccione **Controles de la seguridad** y luego seleccione la subdivisión **Control de aplicaciones**.

4. Haga clic en el botón **Análisis estático**.

   Se abre la ventana **Análisis de la lista de permisos de acceso**. En la parte izquierda de la ventana se muestra una lista de usuarios basada en datos de Active Directory.

5. Seleccione un usuario de la lista.

   La parte derecha de la ventana muestra las categorías de aplicaciones asignadas a este usuario.

6. Para ver los archivos ejecutables que el usuario no está autorizado a ejecutar, en la ventana **Análisis de la lista de permisos de acceso** haga clic en el botón **Ver archivos**.

   Una ventana se abre, en la que se muestra una lista de archivos ejecutables prohibidos.

7. Para ver la lista de archivos ejecutables incluidos en una categoría, seleccione una categoría de aplicaciones y haga clic en el botón **Ver archivos de la categoría**.

   Se abre una ventana que muestra una lista de archivos ejecutables incluidos en la categoría de aplicaciones.

## Consulta del registro de aplicaciones

Kaspersky Security Center realiza un inventario de todo el software instalado en los dispositivos administrados.

El Agente de red elabora una lista de las aplicaciones instaladas en un dispositivo Windows o Linux y la transmite al Servidor de administración. Para los dispositivos cliente basados en Windows, el Agente de red recibe la mayor parte de la información sobre las aplicaciones instaladas del registro de Windows. Para los dispositivos cliente basados en Linux, los administradores de paquetes brindan información al Agente de red sobre las aplicaciones instaladas.

*Para visualizar el registro de las aplicaciones instaladas en dispositivos cliente,*

En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Registro de aplicaciones**.

En el espacio de trabajo de la carpeta **Registro de aplicaciones**, verá una lista con las aplicaciones instaladas en los dispositivos cliente y en el Servidor de administración.

Puede ver los detalles de cualquier aplicación al abrir su menú contextual y seleccionar **Propiedades**. La ventana de propiedades de la aplicación muestra los detalles de la aplicación e información acerca de sus archivos ejecutables, además de una lista de dispositivos en los que está instalada la aplicación.

Utilice el menú contextual de cualquiera de las aplicaciones de la lista para hacer lo siguiente:

- Agregar la aplicación a una categoría de aplicaciones.
- Asignar una etiqueta a la aplicación.
- Exportar la lista de aplicaciones a un archivo CSV o TXT.
- Ver las propiedades de la aplicación seleccionada: el nombre del proveedor, el número de versión, la lista de archivos ejecutables, la lista de dispositivos en los que la aplicación está instalada, la lista de actualizaciones de software disponibles, o la lista de vulnerabilidades de software detectadas y más.

Para visualizar aplicaciones que cumplan con criterios especificados, puede usar los campos de filtrado en el espacio de trabajo de la carpeta **Registro de aplicaciones**.

En la ventana de propiedades del dispositivo seleccionado de la sección **Registro de aplicaciones**, puede ver la lista de aplicaciones instaladas en el dispositivo.

### Generación de un informe sobre las aplicaciones instaladas

En el espacio de trabajo **Registro de aplicaciones** puede hacer clic en el botón **Ver informe sobre aplicaciones instaladas** para generar un informe sobre el software instalado, en el que encontrará estadísticas detalladas como el número de dispositivos en los que cada aplicación está presente. El informe, que se abre en la página **Informe sobre aplicaciones instaladas**, contendrá información tanto sobre las aplicaciones de Kaspersky como sobre las de terceros. Para limitar la información a las aplicaciones de Kaspersky instaladas en los dispositivos cliente, en la lista **Resumen**, seleccione AO Kaspersky Lab.

La información sobre las aplicaciones de Kaspersky y de terceros instaladas en los dispositivos que se encuentran conectados a Servidores de administración secundarios y virtuales también se almacena en el registro de aplicaciones del Servidor de administración principal. Una vez que agregue los datos de los Servidores de administración secundarios y virtuales, haga clic en el botón **Ver informe sobre aplicaciones instaladas**; encontrará la información en la página **Informe sobre aplicaciones instaladas** que se abrirá.

*Para agregar la información de los Servidores de administración secundarios y virtuales al informe sobre aplicaciones instaladas:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la pestaña **Informes**.
3. En la pestaña **Informes**, seleccione **Informe sobre aplicaciones instaladas**.
4. Seleccione **Propiedades** en el menú contextual del informe.

   Se abre la ventana **Propiedades: Informe sobre aplicaciones instaladas**.
5. En la sección **Jerarquía de servidores de administración**, seleccione la casilla de verificación **Incluir datos de servidores de administración secundarios y virtuales**.
6. Haga clic en **Aceptar**.

La información de los Servidores de administración secundarios y virtuales se incluirá en el **Informe sobre aplicaciones instaladas**.

## Modificación de la hora de inicio del inventariado de software

Kaspersky Security Center realiza un inventario de todo el software instalado en los dispositivos cliente administrados que ejecutan Windows.

El Agente de red elabora una lista de las aplicaciones instaladas en un dispositivo y luego transmite la lista al Servidor de administración. La información de las aplicaciones instaladas proviene del Registro de Windows; el Agente de red recibe estos datos automáticamente.

De manera predeterminada, para no malgastar los recursos del dispositivo, el Agente de red comienza a recibir información sobre las aplicaciones instaladas cuando el servicio del Agente de red lleva ya diez minutos en ejecución.

*Para modificar el tiempo que transcurre entre que se inicia el servicio del Agente de red y se realiza el inventario de software en un dispositivo:*

1. Abra el registro del sistema de un dispositivo en el que esté instalado el Agente de red (por ejemplo, de forma local con el comando regedit en el menú **Iniciar** → **Ejecutar**).
2. Vaya al siguiente archivo:
   - Para sistemas de 32 bits:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
   - Para sistemas de 64 bits:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentF
3. Para la clave KLINV_INV_COLLECTOR_START_DELAY_SEC, establezca el valor deseado en segundos.
   De manera predeterminada, el valor es 600 segundos.
4. Reinicie el servicio del Agente de red.

Se modifica el tiempo que transcurre entre que se inicia el servicio del Agente de red y se realiza el inventario de software.

## Acerca de la administración de claves de licencia de aplicaciones de terceros

Kaspersky Security Center le permite realizar un seguimiento del uso de la clave de licencia para aplicaciones de terceros instaladas en los dispositivos administrados. La lista de aplicaciones para las que puede realizar un seguimiento del uso de la clave de licencia se obtiene del registro de aplicaciones. Para cada clave de licencia, puede especificar y rastrear la violación de las siguientes restricciones:

- Número máximo de dispositivos en los que puede instalarse la aplicación que usa esta clave de licencia
- Fecha de caducidad de la clave de licencia

Kaspersky Security Center no comprueba si usted especifica o no una clave de licencia real. Solo puede realizar un seguimiento de las restricciones que especifique. Si se viola una de las restricciones que impone a una clave de licencia del grupo de aplicaciones, el Servidor de administración registra un evento informativo, de advertencia o de error funcional.

Las claves de licencia están vinculadas a grupos de aplicaciones. Un grupo de aplicaciones es un grupo de aplicaciones de terceros que se combinan según un criterio o varios criterios. Puede definir aplicaciones por el nombre de la aplicación, su versión, proveedor y etiqueta. Se agrega una aplicación al grupo si se cumple al menos uno de los criterios. Para cada grupo de aplicaciones, puede vincular varias claves de licencia, pero cada clave de licencia puede vincularse a un solo grupo de aplicaciones.

Para hacer un seguimiento del uso de claves de licencia, también puede utilizar el Informe sobre el estado de los grupos de aplicaciones con licencia. Este informe proporciona información sobre el estado actual de los grupos de aplicaciones con licencia, que incluyen:

- Número de instalaciones de claves de licencia en cada grupo de aplicaciones
- Número de claves de licencia en uso y claves de licencia vacantes
- Lista detallada de aplicaciones con licencia instaladas en los dispositivos administrados

Las herramientas para la administración de claves de licencia de aplicaciones de terceros se encuentran en la subcarpeta **Uso de licencias de terceros** (**Avanzado** → **Administración de aplicaciones** → **Uso de licencias de terceros**). En esta subcarpeta, puede crear grupos de aplicaciones, agregar claves de licencia y generar el Informe sobre los estados de los grupos de aplicaciones con licencia.

Las herramientas para operar con las claves de licencia de aplicaciones de terceros solo están disponibles si habilitó la opción Administración de vulnerabilidades y parches en la ventana **Configurar interfaz**.

## Crear grupos de aplicaciones con licencia

*Para crear un grupo de aplicaciones con licencia:*

1. En la carpeta **Avanzado** → **Administración de aplicaciones** en el árbol de la consola, seleccione la subcarpeta **Uso de licencias de terceros**.
2. Haga clic en el botón **Agregar un grupo de aplicaciones con licencia** para ejecutar Asistente para agregar grupos de aplicaciones con licencia.

   Inicia el Asistente para agregar grupos de aplicaciones con licencia.

3. En el paso **Detalles del grupo de aplicaciones con licencia**, especifique qué aplicaciones desea incluir en el grupo de aplicaciones:

   - **Nombre del grupo de aplicaciones con licencia**
   - **Controlar la infracción de restricciones**

     Si se viola una de las restricciones que impone a una clave de licencia del grupo de aplicaciones, el Servidor de administración registra un evento informativo, de advertencia o de error funcional:

     - Evento informativo: **El límite de instalaciones está por alcanzarse (se consumió más del 95 %) en uno de los grupos de aplicaciones con licencia**
     - Evento de advertencia: **El límite de instalaciones está por excederse en uno de los grupos de aplicaciones con licencia**
     - Evento de error funcional: **Límite de instalaciones excedido en uno de los grupos de aplicaciones con licencia**

       Un evento se registra solo una vez, cuando se cumple la condición establecida. La próxima vez, el mismo evento puede registrarse solo cuando el número de instalaciones regrese a un nivel normal y luego el evento vuelva a ocurrir. Un evento no se puede registrar más de una vez por hora.

   - **Criterios para agregar las aplicaciones detectadas a este grupo de aplicaciones con licencia**

     Especifique criterios para definir qué aplicaciones desea incluir en el grupo de aplicaciones. Puede definir aplicaciones por el nombre de la aplicación, su versión, proveedor y etiqueta. Debe especificar al menos un criterio. Se agrega una aplicación al grupo si se cumple al menos uno de los criterios.

4. En el paso **Ingresar datos sobre las claves de licencia existentes**, especifique las claves de licencia que desea rastrear. Seleccione la opción **Controlar si se excede el límite de licencia** y luego agregue las claves de licencia:

   a. Haga clic en el botón **Agregar**.

   b. Seleccione la clave de licencia que desea agregar y haga clic en el botón **Aceptar**. Si la clave de licencia requerida no aparece en la lista, haga clic en el botón **Agregar** y luego especifique las propiedades de la clave de licencia.

5. En el paso **Agregar un grupo de aplicaciones con licencia**, haga clic en el botón **Finalizar**.

Se crea y se muestra un grupo de aplicaciones con licencia en la carpeta **Uso de licencias de terceros**.

## Administración de claves de licencia para grupos de aplicaciones con licencia

*Para crear una clave de licencia para un grupo de aplicaciones con licencia:*

1. En la carpeta **Avanzado** → **Administración de aplicaciones** en el árbol de la consola, seleccione la subcarpeta **Uso de licencias de terceros**.

2. En el espacio de trabajo de la carpeta **Uso de licencias de terceros**, haga clic en el botón **Administrar claves de licencia de aplicaciones con licencia**.

   Se abre la ventana **Administración de claves de licencia en aplicaciones con licencia**.

3. En la ventana **Administración de claves de licencia en aplicaciones con licencia**, haga clic en el botón **Agregar**.

   Se abre la ventana **Clave de licencia**.

4. En la ventana **Clave de licencia**, especifique las propiedades de la clave de licencia y las restricciones que esta impone al grupo de aplicaciones con licencia.

   - **Nombre**. Nombre de la clave de licencia.
   - **Comentario**. Notas sobre la clave de licencia seleccionada.
   - **Restricción**. Número de dispositivos en los que puede instalarse la aplicación que usa esta clave de licencia.
   - **Vence**. Fecha de vencimiento de la clave de licencia.

Las claves de licencia creadas se muestran en la ventana **Administración de claves de licencia en aplicaciones con licencia**.

*Para aplicar una clave de licencia a un grupo de aplicaciones con licencia:*

1. En la carpeta **Avanzado → Administración de aplicaciones** en el árbol de la consola, seleccione la subcarpeta **Uso de licencias de terceros**.

2. En la carpeta **Uso de licencias de terceros**, seleccione un grupo de aplicaciones con licencia al cual desea aplicar una clave de licencia.

3. Seleccione **Propiedades** del menú contextual del grupo de aplicaciones con licencia.

   Se abre la ventana de propiedades del grupo de aplicaciones con licencia.

4. En la ventana de propiedades del grupo de aplicaciones con licencia, en la sección **Claves de licencia**, seleccione **Controlar si se excede el límite de licencia**.

5. Haga clic en el botón **Agregar**.

   Se abre la ventana **Seleccionar una clave de licencia**.

6. En la ventana **Seleccionar una clave de licencia**, seleccione una clave de licencia que desee aplicar a un grupo de aplicaciones con licencia.

7. Haga clic en **Aceptar**.

Las restricciones impuestas a un grupo de aplicaciones con licencia y especificadas en la clave de licencia también se aplicarán al grupo de aplicaciones con licencia seleccionado.

## Inventario de archivos ejecutables

Puede obtener una lista de los archivos ejecutables almacenados en los dispositivos administrados. Para hacer un inventario de los archivos ejecutables, debe crear una tarea de inventario.

La función de inventario de archivos ejecutables está disponible para las siguientes aplicaciones:

- Kaspersky Endpoint Security para Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization 4.0 Light Agent y versiones posteriores

Kaspersky Security Center puede recibir un máximo de 150 000 archivos ejecutables de cada dispositivo cliente. Habiendo alcanzado este límite, Kaspersky Security Center no puede recibir ningún archivo nuevo.

Antes de comenzar, habilite las notificaciones sobre la ejecución de aplicaciones en la directiva de Kaspersky Endpoint Security y en la directiva del Agente de red para poder transferir datos al Servidor de administración.

*Para habilitar las notificaciones sobre la ejecución de aplicaciones:*

- Abra los ajustes de la directiva de Kaspersky Endpoint Security y, a continuación, haga lo siguiente:
  1. Vaya a **Configuración general** → **Informes y repositorios**.
  2. En la sección **Transferencia de datos al Servidor de administración**, marque la casilla **Acerca de las aplicaciones iniciadas**.
  3. Guarde sus cambios.
- Abra los ajustes de la directiva del Agente de red y, a continuación, haga lo siguiente:
  1. Vaya a la sección **Repositorios**.
  2. Marque la casilla **Detalles de las aplicaciones instaladas**.
  3. Guarde sus cambios.

*Para crear una tarea que haga un inventario de los archivos ejecutables instalados en los dispositivos cliente:*

1. En el árbol de la consola, seleccione la carpeta **Tareas**.
2. En el espacio de trabajo de la carpeta **Tareas**, haga clic en el botón **Nueva tarea**.

   Se inicia el Asistente para crear nueva tarea.
3. En la ventana **Seleccione el tipo de tarea** del asistente, seleccione **Kaspersky Endpoint Security** como el tipo de tarea; a continuación, seleccione **Inventario** como subtipo de tarea y haga clic en **Siguiente**.
4. Siga el resto de instrucciones del asistente.

   Una vez que haya finalizado el asistente, se crea una tarea de inventario para Kaspersky Endpoint Security. La tarea nueva se muestra en la lista de tareas del espacio de trabajo de la carpeta **Tareas**.

En el espacio de trabajo de la carpeta **Archivos ejecutables** se muestra una lista de los archivos ejecutables que se detectaron en los dispositivos cliente durante el inventario.

Durante el inventario, la aplicación detecta archivos ejecutables en los formatos siguientes: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR, y archivos de HTML.

## Visualización de información sobre archivos ejecutables

*Para visualizar una lista de todos los archivos ejecutables detectados en dispositivos cliente,*

En la carpeta **Administración de aplicaciones** del árbol de la consola, seleccione la subcarpeta **Archivos ejecutables**.

En el espacio de trabajo de la carpeta **Archivos ejecutables**, se muestra una lista de los archivos ejecutables que se ejecutaron en los dispositivos o que se detectaron mientras se ejecutaba la tarea de inventario de Kaspersky Endpoint Security para Windows.

Para visualizar los datos en archivos ejecutables que cumplen criterios especificados, puede usar el filtrado.

*Para visualizar las propiedades de un archivo ejecutable,*

En el menú contextual del archivo, seleccione **Propiedades**.

Se abre una ventana que contiene información del archivo ejecutable, junto con una lista de dispositivos en los que se ha detectado el archivo ejecutable.

# Supervisión e informes

Esta sección describe las capacidades de supervisión e informes de Kaspersky Security Center. Estas prestaciones permiten obtener una visión general de la infraestructura, ver los estados de protección y acceder a información estadística.

Después del despliegue de Kaspersky Security Center o durante la operación, puede configurar las funciones de supervisión e informes para que se adapten mejor a sus necesidades.

- **Semáforo**

  La Consola de administración le permite evaluar rápidamente el estado actual de Kaspersky Security Center y dispositivos administrados al comprobar los semáforos.

- **Estadísticas**

  Las estadísticas sobre el estado del sistema de protección y los dispositivos administrados se muestran en paneles de información que se pueden personalizar.

- **Informes**

  La función Informes permite obtener información numérica detallada sobre la seguridad de la red de la organización. La información puede guardarse en un archivo, imprimirse o enviarse por correo electrónico.

- **Eventos**

Las selecciones de eventos brindan una vista en pantalla de distintos conjuntos de eventos, que se toman de la base de datos del Servidor de administración y se identifican con un nombre. Estos conjuntos de eventos se agrupan y clasifican de distintas maneras:

- Por nivel de importancia: **Eventos críticos**, **Errores funcionales**, **Advertencias** y **Eventos informativos**
- Por fecha: **Eventos recientes**
- Por tipo: **Solicitudes de usuario** y **Eventos de auditoría**

Puede usar los ajustes disponibles en la interfaz de Kaspersky Security Center Web Console para ver y crear selecciones de eventos definidas por el usuario.

# Procedimiento: Supervisión y generación de informes

En esta sección se describe un escenario para configurar la característica de supervisión y generación de informes de Kaspersky Security Center.

## Requisitos previos

Cuando Kaspersky Security Center se haya implementado en la red de su organización, podrá supervisar su funcionamiento y generar informes al respecto.

## Etapas

El proceso de supervisar la red de una organización y generar informes se divide en etapas:

1. **Configurar cambios de estado para los dispositivos**

   Obtenga información sobre la configuración que define la asignación de estados del dispositivo según las condiciones específicas. Al cambiar estas configuraciones, puede cambiar la cantidad de eventos con niveles de importancia *Crítica* o *Advertencia*.

   Al configurar la conmutación de estados de los dispositivos, asegúrese de que la nueva configuración no entre en conflicto con las directivas de seguridad de la información de su organización y que pueda reaccionar a eventos de seguridad importantes en la red de su organización de manera oportuna.

2. **Configurar las notificaciones sobre los eventos que suceden en los dispositivos cliente**

   Configure la notificación (por correo electrónico, SMS o ejecutando un archivo ejecutable) de eventos en dispositivos cliente en función de las necesidades de su organización.

3. **Cambiar el modo en que la red de seguridad responde al evento Brote de virus**

   Para ajustar la respuesta de la red a eventos nuevos, puede modificar los umbrales específicos en las propiedades del Servidor de administración. También puede crear una directiva más estricta que se activará o crear una tarea que se ejecutará cuando ocurra este evento.

4. **Administración de estadísticas**

   Configure la visualización de estadísticas en función de las necesidades de su organización.

5. **Controlar el estado de seguridad de la red de la organización**

   Para revisar el estado de seguridad de la red de su organización, puede seguir cualquiera de estos métodos:

- En el espacio de trabajo del nodo **Servidor de administración**, en la pestaña **Estadísticas**, abra la pestaña de segundo nivel (página) **Estado de protección** y consulte el panel de información **Estado de la protección en tiempo real**
- Genere y revise el **Informe del estado de la protección**
- Genere y revise el **Informe de errores**

6. **Buscar dispositivos cliente que no se encuentren protegidos**

   Para localizar dispositivos cliente que no están protegidos, vaya al espacio de trabajo del nodo **Servidor de administración**, en la pestaña **Estadísticas**, abra la pestaña de segundo nivel (página) **Estado de protección** y consulte el panel de información **Historial de detección de dispositivos nuevos en red**. También puede generar y revisar el **Informe del despliegue de la protección**.

7. **Controlar la protección de los dispositivos cliente**

   Para comprobar la protección de dispositivos cliente, vaya al espacio de trabajo del nodo **Servidor de administración**, en la pestaña **Estadísticas**, abra la pestaña de segundo nivel (página) **Despliegue** o **Estadísticas de amenazas** y consulte los paneles de información correspondientes. También puede iniciar y revisar la selección de **Eventos críticos**.

8. **Evaluar y limitar el impacto de los eventos en la base de datos**

   Se transfiere la información sobre eventos que ocurren durante el funcionamiento de aplicaciones administradas de un dispositivo cliente y se registra en la base de datos del Servidor de administración. Para reducir la carga del Servidor de administración, evalúe y limite la cantidad de eventos que se guardan como máximo en la base de datos.

   Para evaluar la carga de eventos en la base de datos, calcule el espacio de la base de datos. También puede limitar el número máximo de eventos para evitar el desbordamiento de la base de datos.

9. **Controlar la información de las licencias**

   Para consultar la información de la licencia, vaya al espacio de trabajo del nodo **Servidor de administración**, en la pestaña **Estadísticas**, abra la pestaña de segundo nivel (página) **Despliegue** y consulte el panel de información **Uso de clave de licencia**. También puede generar y revisar el **Informe de uso de claves de licencia**.

### Resultados

Al concluir este escenario, podrá mantenerse al corriente de la protección de su red y estará en condiciones de planificar medidas de protección adicionales.

# Controlar los semáforos y los eventos registrados en la Consola de Administración

La Consola de administración le permite evaluar rápidamente el estado actual de Kaspersky Security Center y dispositivos administrados al comprobar los semáforos. Los semáforos se muestran en el espacio de trabajo del nodo **Servidor de administración**, en la pestaña **Supervisión**. La pestaña proporciona seis paneles de información con semáforos y eventos registrados. Un semáforo es una barra vertical de color en el lado izquierdo de un panel. Cada panel con un semáforo equivale a un alcance funcional específico de Kaspersky Security Center (ver la tabla a continuación).

Alcances cubiertos por semáforos en la Consola de administración

| Nombre del panel | Alcance del semáforo |
|---|---|
| **Despliegue** | Instalación del Agente de red y aplicaciones de seguridad en dispositivos en una red de la organización |
| **Esquema de administración** | Estructura de grupos de administración. Análisis de la red. Reglas de movimiento de dispositivos |
| **Opciones de protección** | Funcionalidad de la aplicación de seguridad: estado de la protección, análisis del malware |
| **Actualización** | Actualizaciones y parches |
| **Supervisión** | Estado de protección |
| **Servidor de administración** | Funciones y propiedades del Servidor de administración |

Cada semáforo puede prenderse en cualquiera de estos cinco colores (ver la tabla a continuación). El color de un semáforo depende del estado actual de Kaspersky Security Center y de los eventos que se registraron.

Códigos de colores de los semáforos

| Estado | Color del semáforo | Significado del color del semáforo |
|---|---|---|
| Informativo | Verde | No se requiere intervención del administrador. |
| Advertencia | Amarillo | Se requiere intervención del administrador. |
| Crítico | Rojo | Se han detectado graves problemas. Intervención del administrador requerida para solucionarlos. |
| Informativo | Azul claro | Se han registrado eventos que no están relacionados con amenazas posibles o reales a la seguridad de dispositivos administrados. |
| Informativo | Gris | Los detalles de eventos no están disponibles o todavía no se han recuperado. |

El objetivo del administrador es mantener los semáforos en todos los paneles de información en la pestaña **Supervisión** en verde.

Los paneles de información también muestran los eventos registrados que afectan los semáforos y el estado de Kaspersky Security Center (vea la siguiente tabla).

Nombre, descripción y color de semáforo de los eventos registrados

| Color del semáforo | Nombre que se muestra para el tipo de evento | Tipo de evento | Descripción |
|---|---|---|---|
| Rojo | **La licencia caducó en %1 dispositivo(s)** | IDS_AK_STATUS_LIC_EXPAIRED | Este tipo de eventos ocurre cuando caduca la licencia comercial.<br>Kaspersky Security Center verifica una vez al día si la licencia ha caducado en los dispositivos.<br>Cuando caduca la licencia comercial, Kaspersky Security Center solo brinda acceso a las funciones básicas.<br>Para seguir usando Kaspersky Security Center, renueve su licencia comercial. |
| Rojo | **La aplicación de seguridad no se está ejecutando en %1 dispositivo(s)** | IDS_AK_STATUS_AV_NOT_RUNNING | Este tipo de evento ocurre cuando la aplicación de seguridad instalada en el dispositivo no se está ejecutando.<br>Asegúrese de que Kaspersky Endpoint Security se esté ejecutando en el dispositivo. |
| Rojo | **La protección está deshabilitada en: %1 dispositivo(s)** | IDS_AK_STATUS_RTP_NOT_RUNNING | Este tipo de evento ocurre cuando la aplicación de seguridad del dispositivo ha estado deshabilitada por un tiempo superior al especificado.<br>Revise el estado de la protección en tiempo real en el dispositivo y asegúrese de que todos los componentes de protección que necesite estén habilitados. |

| Color del semáforo | Nombre que se muestra para el tipo de evento | Tipo de evento | Descripción |
|---|---|---|---|
| Rojo | **Se detectó una vulnerabilidad de software en los dispositivos** | IDS_AK_STATUS_VULNERABILITIES_FOUND | Este tipo de evento ocurre cuando la tarea *Buscar vulnerabilidades y actualizaciones requeridas* ha detectado vulnerabilidades con el nivel de gravedad especificado en las aplicaciones instaladas en el dispositivo.<br>Consulte la lista de actualizaciones disponibles en la subcarpeta **Actualizaciones de software** de la carpeta **Administración de aplicaciones**. Esta carpeta contiene una lista de las actualizaciones obtenidas por el Servidor de administración para las aplicaciones de Microsoft y para los productos de otros proveedores de software que pueden distribuirse a los dispositivos.<br>Tras revisar la información sobre las actualizaciones disponibles, instálelas en el dispositivo. |
| Rojo | **Se han registrado eventos críticos en el Servidor de administración** | IDS_AK_STATUS_EVENTS_OCCURED | Este tipo de evento ocurre cuando se detectan eventos críticos del Servidor de administración.<br>Revise la lista de eventos almacenados en el Servidor de administración y luego corrija los eventos críticos uno por uno. |
| Rojo | **Eventos de error registrados en el Servidor de administración** | IDS_AK_STATUS_ERROR_EVENTS_OCCURED | Este tipo de evento ocurre cuando se registran errores inesperados en el lado del Servidor de administración.<br>Revise la lista de eventos almacenados en el Servidor de administración y luego corrija los errores uno por uno. |
| Rojo | **Se perdió la conexión con %1 dispositivo(s)** | IDS_AK_STATUS_ADM_LOST_CONTROL1 | Este tipo de evento ocurre cuando se pierde la conexión entre el Servidor de administración y el dispositivo.<br>Revise la lista de dispositivos desconectados e intente volver a conectarlos. |
| Rojo | **%1 dispositivo/s no se ha conectado al Servidor de administración en mucho tiempo** | IDS_AK_STATUS_ADM_NOT_CONNECTED1 | Este tipo de evento ocurre cuando el dispositivo se encuentra apagado y, debido a ello, no se ha conectado al Servidor de administración en el período de tiempo especificado.<br>Asegúrese de que el dispositivo esté encendido y compruebe que el Agente de red se esté ejecutando. |
| Rojo | **Hay %1 dispositivo(s) cuyo estado no es Sin inconvenientes** | IDS_AK_STATUS_HOST_NOT_OK | Este tipo de evento ocurre cuando el estado *Sin inconvenientes* del dispositivo conectado al Servidor de administración cambia a *Crítico* o a *Advertencia*.<br>Puede buscar una solución a este problema con la Utilidad de diagnóstico remoto de Kaspersky Security Center. |
| Rojo | **Las bases de datos están desactualizadas en: %1 dispositivo(s)** | IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED | Este tipo de evento ocurre cuando las bases de datos antivirus no se han actualizado en el dispositivo dentro del intervalo de tiempo especificado.<br>Siga las instrucciones para actualizar las bases de datos de Kaspersky. |

| Color del semáforo | Nombre que se muestra para el tipo de evento | Tipo de evento | Descripción |
|---|---|---|---|
| Rojo | **Dispositivo/s donde no se ha realizado una comprobación de actualizaciones de Windows Update en mucho tiempo: %1** | IDS_AK_STATUS_WUA_DATA_OBSOLETE | Este tipo de evento ocurre cuando la tarea *Realizar la sincronización con Windows Update* no se ha ejecutado en el intervalo de tiempo especificado.<br>Siga las instrucciones para sincronizar las actualizaciones de Windows Update con el Servidor de administración. |
| Rojo | **Es necesario instalar %1 complemento(s) para Kaspersky Security Center** | IDS_AK_STATUS_PLUGINS_REQUIRED2 | Este tipo de evento ocurre cuando se deben instalar complementos adicionales para las aplicaciones de Kaspersky.<br>Descargue e instale los complementos de administración necesarios para la aplicación Kaspersky desde la página web del Servicio de soporte técnico de Kaspersky. |

# Trabajo con informes, estadísticas y notificaciones

Esta sección provee información sobre cómo trabajar con informes, estadísticas y selecciones de eventos y dispositivos en Kaspersky Security Center y, además, sobre cómo configurar las notificaciones del Servidor de administración.

## Trabajo con informes

Los informes en Kaspersky Security Center tienen información acerca del estado de los dispositivos administrados. Los informes se generan basándose en la información almacenada en el Servidor de administración. Puede crear informes para los siguientes tipos de objetos:

- Para selecciones de dispositivos creados según una configuración específica.
- Para grupos de administración.
- Para dispositivos específicos de grupos de administración diferentes.
- Para todos los dispositivos de la red (en el informe de despliegue).

La aplicación incluye una selección de plantillas de informes estándar. También se pueden crear plantillas de informes personalizadas. Los informes se muestran en la ventana principal de la aplicación, en la carpeta **Servidor de administración** del árbol de consola.

### Crear una plantilla de informe

*Para crear una plantilla de informe:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la pestaña **Informes**.
3. Haga clic en el botón **Nueva plantilla de informe**.

Se abre el Asistente de nueva plantilla de informe. Siga las instrucciones del asistente.

Una vez que el Asistente finaliza su operación, la plantilla de informe recién creada se agrega a la carpeta **Servidor de administración** seleccionada del árbol de consola. Puede utilizar esta plantilla para generar y ver informes.

## Ver y editar las propiedades de una plantilla de informe

Puede ver y editar las propiedades básicas de las plantillas de informe (por ejemplo, el nombre de las plantillas o los campos que se muestran en los informes).

*Para ver y editar las propiedades de una plantilla de informe:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la pestaña **Informes**.
3. En la lista de plantillas de informe, seleccione la plantilla de informe requerida.

4. En el menú contextual de la plantilla de informe seleccionada, seleccione **Propiedades**.

   Como una alternativa, primero puede generar el informe y después hacer clic en el botón **Abrir las propiedades de la plantilla del informe** o el botón **Configurar columnas del informe**.

5. En la ventana que se abre, edite las propiedades de la plantilla de informe. Las propiedades de cada informe pueden contener solo algunas de las secciones que se describen a continuación.

   - Sección **General**:

     - Nombre de la plantilla de informe

     - Cantidad máxima de entradas para mostrar

       Si esta opción está habilitada, la tabla con los datos detallados del informe mostrará, como máximo, el número de entradas indicado aquí.

       Las entradas del informe se ordenan primero siguiendo las reglas especificadas en la sección **Campos** → **Campos Detalles** de las propiedades de la plantilla de informe, y luego se conservan solo las primeras de las entradas resultantes. El encabezado de la tabla con los datos detallados del informe indica el número de entradas mostradas y el total de entradas disponibles que coinciden con otros parámetros de la plantilla del informe.

       Si deshabilita esta opción, se mostrarán todas las entradas disponibles en la tabla con los datos detallados del informe. No recomendamos deshabilitar esta opción. Al limitar el número de entradas que se muestran en un informe, se aminora la carga en el sistema de administración de bases de datos y se reduce el tiempo requerido para generar y exportar el informe. Algunos de los informes contienen demasiadas entradas. En tales casos, no es sencillo leer y analizar todas las entradas. Además, cuando se genera un informe de este tipo, se corre el riesgo de que el dispositivo se quede sin memoria; de ocurrir este problema, no será posible siquiera ver el informe.

       Esta opción está activada de forma predeterminada. El valor predeterminado es 1000.

     - Versión de impresión

       La salida del informe está optimizada para la impresión: los caracteres de espacio se añaden entre algunos valores para una mejor visibilidad.

       Esta opción está activada de forma predeterminada.

   - Sección **Campos**.

     Seleccione los campos que se mostrarán en el informe y el orden de estos campos, y configure si cada uno de los campos debe clasificar y filtrar la información en el informe.

   - Sección **Intervalo de tiempo**.

     Modificar el período del informe. Los valores disponibles son los siguientes:

     - Entre dos fechas específicas

     - Desde una fecha específica hasta la fecha de creación del informe

     - Desde cierta cantidad de días antes de la creación del informe hasta la fecha de creación del informe

   - **Grupo**, **Selección de dispositivos** o sección **Dispositivos**.

     Cambie el conjunto de dispositivos cliente para los que se crea el informe. Solo una de estas secciones puede estar presente, dependiendo de la configuración especificada durante la creación de la plantilla del informe.

- Sección **Configuración**.

  Cambiar la configuración del informe. El conjunto exacto de ajustes depende del informe específico.

- Sección **Seguridad**. Heredar configuración del Servidor de administración

  Si esta opción está activada, la configuración de seguridad del informe se hereda del Servidor de administración.

  Si esta opción está desactivada, puede configurar los ajustes de seguridad para el informe. Puede asignar una función a un usuario o un grupo de usuarios o asignar permisos a un usuario o un grupo de usuarios, según se aplique al informe.

  Esta opción está activada de forma predeterminada.

  La sección **Seguridad** está disponible si la casilla **Mostrar secciones de configuración de seguridad** está seleccionada en la ventana de configuración de la interfaz.

- Sección **Jerarquía de servidores de administración**:

  - Incluir datos de servidores de administración secundarios y virtuales

    Cuando esta opción se encuentra habilitada, el informe incluye información de los servidores de administración secundarios y virtuales que están subordinados al Servidor de administración para el cual se ha creado la plantilla de informe.

    Deshabilite esta opción si solo desea ver datos del Servidor de administración con el que está trabajando.

    Esta opción está activada de forma predeterminada.

  - Hasta el nivel de anidamiento

    El informe incluirá datos de los servidores de administración secundarios y virtuales que se encuentren <n> o más niveles de anidamiento por debajo del Servidor de administración con el que se esté trabajando, siendo <n> el valor especificado.

    El valor predeterminado es 1. Puede cambiar este valor si necesita recuperar información de servidores de administración secundarios que se encuentren aún más abajo en el árbol.

  - Intervalo de espera de datos (min)

    Antes de generar el informe, el Servidor de administración para el que se haya creado la plantilla de informe esperará, durante el tiempo especificado, a que los servidores de administración secundarios le envíen datos. Transcurrido este período de espera, el Servidor generará el informe aunque no haya recibido información de los servidores de administración secundarios. En lugar de los datos reales, el informe muestra **N/D** (no disponible) o, si la opción **Datos de caché de los Servidores de administración secundarios** está habilitada, los datos tomados de la caché.

    El valor predeterminado es 5 (minutos).

  - Almacenar en caché los datos de los servidores de administración secundarios

Los servidores de administración secundarios transfieren datos periódicamente al Servidor de administración para el que se ha creado la plantilla de informe. Una vez allí, los datos transferidos se guardan en una caché.

Si, al momento de generar un informe, el Servidor de administración no puede recibir datos de algún Servidor de administración secundario, el informe contendrá los datos de esta caché. La fecha en que los datos se transfirieron a la caché estará indicada en el informe.

Si habilita esta opción, podrá ver datos de los servidores de administración secundarios incluso cuando no se pueda obtener información actualizada. Sin embargo, los datos mostrados podrían ser obsoletos.

Esta opción está deshabilitada de forma predeterminada.

- **Frecuencia de actualización de la caché (h)**

  Los servidores de administración secundarios transfieren datos a intervalos regulares al Servidor de administración para el que se ha creado la plantilla de informe. Puede especificar el largo de este intervalo en horas. Si fija el valor en 0 horas, solamente se transferirá información cuando se genere el informe.

  El valor predeterminado es 0.

- **Transferir información detallada de los servidores de administración secundarios**

  En el informe generado, la tabla con los datos detallados del informe contendrá datos de los servidores de administración secundarios que estén subordinados al Servidor de administración para el cual se haya creado la plantilla de informe.

  Si habilita esta opción, los informes tardarán más tiempo en generarse y habrá más tráfico entre los servidores de administración. Sin embargo, podrá ver toda la información en un solo informe.

  En lugar de habilitar esta opción, podría analizar los datos detallados de un informe para detectar un Servidor de administración secundario con problemas y, hecho esto, generar ese mismo informe únicamente para ese Servidor de administración.

  Esta opción está deshabilitada de forma predeterminada.

## Formato de filtro extendido en plantillas de informes

En Kaspersky Security Center 15.1, puede aplicar el formato de filtro extendido a una plantilla de informe. El formato de filtro extendido es más flexible que el formato predeterminado. Puede crear condiciones de filtrado complejas mediante un conjunto de filtros, que se aplicarán al informe mediante el operador lógico "O" durante su creación, tal como se muestra a continuación:

Filtro[1](Campo[1] Y Campo[2]... Y Campo[n]) O Filtro[2](Campo[1] Y Campo[2]... Y Campo[n]) O... Filtro[n](Campo[1] Y Campo[2]... Y Campo[n])

Además, con el formato de filtro extendido, puede establecer un valor para el intervalo de tiempo en un formato de tiempo relativo (por ejemplo, con una condición del tipo "Para los últimos N días") para campos específicos en un filtro. La disponibilidad y los tipos de condiciones de intervalos de tiempo dependen del tipo de plantilla de informe.

## Conversión del filtro al formato extendido

El formato de filtro extendido para las plantillas de informes solo es compatible con Kaspersky Security Center 12 y versiones posteriores. Después de convertir el filtro predeterminado al formato extendido, la plantilla de informe deja de ser compatible con los Servidores de administración de su red que tienen instaladas versiones anteriores de Kaspersky Security Center. La información de estos Servidores de administración no se tomará en cuenta para el informe.

*Para convertir el filtro predeterminado de la plantilla de informe al formato extendido, haga lo siguiente:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la pestaña **Informes**.
3. En la lista de plantillas de informe, seleccione la plantilla de informe requerida.
4. En el menú contextual de la plantilla de informe seleccionada, seleccione **Propiedades**.
5. En la ventana de las propiedades que se abre, seleccione la sección **Campos**.
6. En la pestaña **Campos Detalles**, haga clic en el enlace **Convertir filtro**.
7. En la ventana que se abre, haga clic en el botón **Aceptar**.

   La conversión al formato de filtro extendido es irreversible para la plantilla de informe a la que se aplica. Si hizo clic accidentalmente en el vínculo **Convertir filtro**, puede hacer clic en el botón **Cancelar** de la ventana de propiedades de la plantilla de informe para cancelar los cambios.

8. Para aplicar los cambios, haga clic en el botón **Aceptar** para cerrar la ventana de propiedades de la plantilla de informe.

   Cuando se abre nuevamente la ventana de propiedades de la plantilla de informe, se muestra la nueva sección de **Filtros** disponibles. En esta sección puede configurar el filtro extendido.

## Configuración del filtro extendido

*Para configurar el filtro extendido en las propiedades de la plantilla de informe, haga lo siguiente:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la pestaña **Informes**.
3. En la lista de plantillas de informes, seleccione la plantilla de informe que se había convertido al formato de filtro extendido.
4. En el menú contextual de la plantilla de informe seleccionada, seleccione **Propiedades**.
5. En la ventana de propiedades que se abre, seleccione la sección **Filtros**.

   La sección **Filtros** no se muestra si la plantilla del informe no se ha convertido previamente al formato de filtro extendido.

   En la sección **Filtros** de la ventana de propiedades de la plantilla de informe, puede revisar y modificar la lista de filtros que se aplican al informe. Cada filtro de la lista tiene un nombre único y representa un conjunto de filtros para los campos correspondientes del informe.

6. Abra la ventana de configuración de filtros de alguna de las siguientes formas:

   - Para crear un filtro nuevo, haga clic en el botón **Agregar**.
   - Para modificar el filtro actual, seleccione el filtro requerido y haga clic en el botón **Modificar**.

7. En la ventana que se abre, seleccione y especifique los valores de los campos obligatorios del filtro.
8. Haga clic en el botón **Aceptar** para guardar los cambios y cerrar la ventana.

   Si está creando un filtro nuevo, el nombre del filtro se debe especificar en el campo **Nombre de filtro** antes de hacer clic en el botón **Aceptar**.

9. Para cerrar la ventana de propiedades de la plantilla de informe, haga clic en el botón **Aceptar**.

   El filtro extendido en la plantilla de informe está configurado. Ahora puede crear informes con esta plantilla de informe.

## Crear y ver un informe

*Para crear y ver un informe:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la pestaña **Informes**.
3. En la lista de plantillas de informe, haga doble clic en el modelo de informe que necesite.

   Se visualiza un informe para el modelo seleccionado.

El informe contendrá los siguientes datos:

- El nombre del informe, el tipo de informe, una descripción breve, el período comprendido por el informe e información sobre el grupo de dispositivos para los que se generó el informe.
- Un gráfico con los datos más representativos del informe.
- Una tabla unificada con los indicadores calculados del informe.
- Tabla con datos detallados del informe.

## Guardar un informe

*Para guardar un informe creado:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la pestaña **Informes**.
3. En la lista de plantillas de informe, seleccione la plantilla de informe que necesita.
4. En el menú contextual de la plantilla de informe seleccionada, seleccione **Guardar**.

Se inicia el Asistente para guardar informes. Siga las instrucciones del asistente.

Una vez que el Asistente finalice, la carpeta se abre en el lugar en que se guardó el archivo de informe.

Cuando guarda un informe como un archivo XLS, todas las imágenes relacionadas, como el logotipo y el datagrama, se guardan como archivos separados.

## Crear una tarea de entrega de informes

Los informes se pueden enviar por correo electrónico. El envío de informes en Kaspersky Security Center se realiza mediante la tarea de envío de informes.

*Para crear una tarea de envío para un único informe:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la pestaña **Informes**.
3. En la lista de plantillas de informe, seleccione la plantilla de informe que necesita.
4. En el menú contextual de la plantilla de informe seleccionada, seleccione **Entregar informes**.

   Se inicia el Asistente de creación de tareas de entrega de informes. Siga las instrucciones del asistente.

*Para crear una tarea de envío para varios informes:*

1. En el árbol de consola, seleccione la carpeta **Tareas** en el nodo con el nombre del Servidor de administración correspondiente.
2. En el espacio de trabajo de la carpeta **Tareas**, haga clic en el botón **Crear una tarea**.

   Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente.

   La tarea nueva de entrega de informes se muestra en la carpeta **Tareas** del árbol de consola.

La tarea de envío de informes se crea automáticamente si se especificó la configuración de correo electrónico durante la instalación de Kaspersky Security Center.

### Paso 1. Selección del tipo de tarea

En la ventana **Seleccione el tipo de tarea**, en la lista de tareas seleccione **Entregar informes** como el tipo de tarea.

Haga clic en **Siguiente** para ir al paso siguiente.

### Paso 2. Selección del tipo de informe

En la ventana **Seleccionar el tipo de informe**, en la lista de plantillas de creación de la tarea, seleccionan el tipo de informe.

Haga clic en **Siguiente** para ir al paso siguiente.

### Paso 3. Acciones en un informe

En la ventana **Acción para aplicar a los informes**, especifique los siguientes ajustes:

- **Enviar informes por correo electrónico**

  Si se habilita esta opción, la aplicación enviará los informes generados por correo electrónico.

  Puede configurar el envío de informes por correo electrónico haciendo clic en el enlace **Configuración de notificaciones por correo electrónico**. El enlace estará disponible si se habilita esta opción.

  Si se deshabilita esta opción, la aplicación guardará los informes en la carpeta de almacenamiento especificada.

  Esta opción está deshabilitada de forma predeterminada.

- **Guardar informes en una carpeta compartida**

  Si se habilita esta opción, la aplicación guardará los informes en la carpeta que se especifica en el campo que se encuentra debajo de la casilla. Para guardar informes en una carpeta compartida, especifique la ruta de UNC a la carpeta. En este caso, en la ventana **Seleccionar una cuenta con la que ejecutar la tarea**, debe especificar la cuenta de usuario y contraseña para acceder a esta carpeta.

  Si se deshabilita esta opción, la aplicación no guardará los informes en la carpeta y los enviará por correo electrónico.

  Esta opción está deshabilitada de forma predeterminada.

- **Sobrescribir informes antiguos del mismo tipo**

  Si se habilita esta opción, el nuevo archivo de informe, al iniciarse cada tarea, sobrescribirá archivo guardado en la carpeta de informes al iniciarse la tarea anterior.

  Si se deshabilita esta opción, los archivos de informe no se sobrescribirán. Se guardará un nuevo archivo de informe en la carpeta de informes al ejecutarse cada tarea.

  Esta casilla estará disponible si se selecciona la opción **Guardar informe en carpeta**.

  Esta opción está deshabilitada de forma predeterminada.

- **Especificar cuenta para acceder a la carpeta compartida**

  Si se habilita esta opción, podrá especificar la cuenta bajo la cual se guardará el informe en la carpeta. Si una ruta de UNC a una carpeta compartida se especifica como **Guardar informe en la carpeta** que configura en la ventana **Acción que se tomará con el informe**, debe especificar la cuenta de usuario y contraseña para acceder a esta carpeta.

  Si se deshabilita esta opción, el informe se guardará en la carpeta bajo la cuenta del Servidor de administración.

  Esta casilla estará disponible si se selecciona la opción **Guardar informe en carpeta**.

  Esta opción está deshabilitada de forma predeterminada.

Cuando guarda o envía un informe como un archivo XLS, todas las imágenes relacionadas, como el logotipo y el datagrama, se guardan como archivos separados.

Haga clic en **Siguiente** para ir al paso siguiente.

## Paso 4. Selección de una cuenta para iniciar la tarea

En la ventana **Seleccione una cuenta para ejecutar la tarea**, puede especificar que cuenta usar al ejecutar la tarea. Seleccione una de las siguientes opciones:

- **Cuenta predeterminada**

  La tarea se ejecutará utilizando la misma cuenta que la aplicación que realizará la tarea.

  Esta opción está seleccionada de forma predeterminada.

- **Especificar cuenta**

  Complete los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta con la que se ejecutará la tarea. La cuenta debe tener los derechos necesarios para realizar la tarea.

  - **Cuenta**

    Cuenta con la que se ejecutará la tarea.

  - **Contraseña**

    Contraseña de la cuenta con la que se ejecutará la tarea.

Haga clic en **Siguiente** para ir al paso siguiente.

## Paso 5. Configuración de una programación de tarea

En la página **Configurar programación de tarea**, puede crear una planificación para el inicio de la tarea. Si es necesario, defina la siguiente configuración:

- Inicio programado:

  Seleccione y configure la programación según la cual se ejecutará la tarea.

  - Cada N horas

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

    De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

  - Cada N días

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

    De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

  - Cada N semanas

    La tarea se ejecutará periódicamente, a intervalos regulares, en el día de la semana y a la hora que especifique. Cada ejecución estará separada de la anterior por el número de semanas que indique.

    Por defecto, la tarea se ejecutará cada lunes a la hora actual del sistema.

  - Cada N minutos

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

    De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

  - Diario (no compatible con horario de verano)

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta programación no tiene en cuenta los cambios de horario estacionales. La hora de inicio de la tarea se mantendrá sin cambios incluso si el reloj se atrasa o se adelanta una hora debido al horario de verano.

    No recomendamos usar esta programación. Se la ofrece para mantener la compatibilidad con versiones anteriores de Kaspersky Security Center.

    De forma predeterminada, la tarea se iniciará todos los días a la hora actual del sistema.

  - Semanal

La tarea se ejecutará cada semana en el día y a la hora que indique.

- **Por días de la semana**

  La tarea se ejecutará periódicamente en los días de la semana y a la hora que indique.

  De manera predeterminada, la tarea se ejecutará todos los viernes a las 18:00:00.

- **Mensual**

  La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

  Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

  Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

- **Manual**

  La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

  Esta opción está seleccionada de forma predeterminada.

- **Cada mes en los días especificados de semanas seleccionadas**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  De forma predeterminada, la hora de inicio es a las 18:00 y no se selecciona ningún día del mes.

  Tenga en cuenta que no selecciona una fecha específica en el mes, ni el número de la semana (primera, segunda semana del mes), sino el número de secuencia del día de la semana dentro de un mes. Por ejemplo, si coloca el cursor en la celda **Ma** de la **Primero** fila, significa que la tarea se ejecutará el primer martes de cada mes nuevo.

  Puede seleccionar varios días de la semana.

- **Ante brotes de virus**

  La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para defensa del perímetro
  - Antivirus para sistemas de correo

  Por defecto, están seleccionados todos los tipos de aplicaciones.

  En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- Al completarse otra tarea

  La tarea actual se iniciará después de que se complete otra tarea. Esta opción solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

- Ejecutar tareas no realizadas

  Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

  Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

  Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

  Esta opción está deshabilitada de forma predeterminada.

- Esperar un tiempo definido al azar antes de iniciar la tarea

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

- Limitar el tiempo de espera a esta cantidad de minutos

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

  Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

### Paso 6. Definición del nombre de la tarea

En la ventana **Defina el nombre de la tarea**, especifique el nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales (`"*<>?\:|`).

Haga clic en **Siguiente** para ir al paso siguiente.

### Paso 7. Completar creación de la tarea

En la ventana **Finalizar la creación de la tarea**, haga clic en el botón **Finalizar** para completar el Asistente.

Para que la tarea se inicie en cuanto se cierre el asistente, marque la casilla **Ejecutar la tarea al finalizar el asistente**.

## Administración de estadísticas

Las estadísticas sobre el estado del sistema de protección y los dispositivos administrados se muestran en paneles de información que se pueden personalizar. Las estadísticas se muestran en el espacio de trabajo del nodo del **Servidor de administración** en la pestaña **Estadísticas**. La pestaña contiene algunas pestañas de segundo nivel (páginas). Cada página con pestañas muestra paneles de información con estadísticas, así como vínculos a noticias corporativas y otros materiales de Kaspersky. La información estadística se muestra en paneles de información en forma de tabla o gráfico (de barras o circular). Los datos en los paneles de información se actualizan mientras se ejecuta la aplicación y reflejan el estado actual de la aplicación de protección.

Puede modificar el conjunto de pestañas de segundo nivel en la pestaña **Estadísticas**, el número de paneles de información en cada página con pestañas y el modo de visualización de datos en los paneles de información.

*Para añadir una nueva pestaña de segundo nivel con paneles de información en la pestaña **Estadísticas**:*

1. Haga clic en el botón **Personalizar vista** Ver en la esquina superior derecha de la pestaña **Estadísticas**.

   Se abre la ventana de propiedades de las estadísticas. Esta ventana contiene una lista de las páginas con pestañas que se muestran actualmente en la pestaña **Estadísticas**. En esta ventana, puede cambiar el orden de visualización de las páginas en la pestaña, agregar y quitar páginas e ingresar a la configuración de las propiedades de la página haciendo clic en el botón **Propiedades**.

2. Haga clic en el botón **Agregar**.

   Se abre la ventana de propiedades de una página nueva.

3. Configure la página nueva:

   - En la sección **General**, escriba el nombre de la página.
   - En la sección **Paneles de información**, haga clic en el botón **Agregar** para agregar los paneles de información que se mostrarán en la página.

     Haga clic en el botón **Propiedades** en la sección **Paneles de información** para configurar las propiedades de los paneles de información que se agregaron: nombre, tipo y apariencia del gráfico en el panel, y datos que se usan para crear el gráfico.

4. Haga clic en **Aceptar**.

En la pestaña **Estadísticas** aparece la página con pestañas con los paneles de información que ha añadido. Haga clic en el icono de configuración ( ⚙ ) para proceder instantáneamente a la configuración de la página o de un panel de información seleccionado en esa página.

## Configuración de la notificación de eventos

Kaspersky Security Center le permite seleccionar un método para notificar al administrador sobre los eventos que ocurrieron en dispositivos cliente y configurar las notificaciones:

- Correo electrónico. Cuando ocurre un evento, la aplicación envía una notificación a las direcciones de correo electrónico especificadas. Puede editar el texto de la notificación.
- SMS. Cuando ocurre un evento, la aplicación envía una notificación a los números de teléfono especificados. Puede configurar las notificaciones por SMS para que se envíen a través de la pasarela de correo.
- Archivo ejecutable. Cuando ocurre un evento en un dispositivo, se inicia el archivo ejecutable en la estación de trabajo del administrador. Usando el archivo ejecutable, el administrador puede recibir los parámetros de cualquier evento que haya ocurrido.

*Para configurar notificaciones de eventos que ocurrieron en los dispositivos cliente:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la pestaña **Eventos**.
3. Haga clic en el enlace **Configurar notificaciones y la exportación de eventos** y seleccione el valor **Configurar notificaciones** en la lista desplegable.

   Esto abre la ventana **Propiedades: Eventos**.

4. En la sección **Notificación**, seleccione un método de notificación (por SMS, correo electrónico o al abrir un archivo ejecutable) y configure la notificación:

   - Correo electrónico

La pestaña **Correo electrónico** permite configurar las notificaciones de correo electrónico para eventos.

En el campo **Destinatarios (direcciones de correo electrónico)**, especifique las direcciones de correo electrónico a las que la aplicación enviará notificaciones. Puede especificar varias direcciones en este campo, separándolas con punto y coma.

En el campo **Servidores SMTP**, especifique las direcciones del servidor de correo, separándolas con punto y coma. Puede utilizar los siguientes parámetros:

- Dirección IPv4 o IPv6
- Nombre de la red de Windows (nombre NetBIOS) del dispositivo
- Nombre DNS del servidor SMTP

En el campo **Puerto de los servidores SMTP**, especifique el número de un puerto de comunicación del servidor SMTP. El número de puerto predeterminado es 25.

Si habilita la opción **Buscar registros MX por DNS**, puede utilizar varios registros MX de las direcciones IP para el mismo nombre DNS del servidor SMTP. El mismo nombre DNS puede tener varios registros MX con diferentes valores de prioridad de recepción de mensajes de correo electrónico. El Servidor de administración intenta enviar notificaciones del correo electrónico al servidor SMTP en orden ascendente de prioridad de registros MX. Esta opción está deshabilitada de forma predeterminada.

Si habilita la opción **Buscar registros MX por DNS** y no habilita el uso de la configuración de TLS, le recomendamos que use la configuración de DNSSEC en el dispositivo de su servidor como medida adicional de protección en el envío de notificaciones del correo electrónico.

Haga clic en el enlace **Configuración** para definir más ajustes de notificaciones:

- Nombre del sujeto (nombre del sujeto de un mensaje de correo electrónico)
- Dirección de correo electrónico del remitente
- Configuración de autenticación ESMTP

Debe especificar una cuenta para autenticar en un servidor SMTP si la opción de autenticación de ESMTP está habilitada para el servidor SMTP.

- Configuración de TLS para el servidor SMTP:
  - **No utilizar TLS**

    Puede seleccionar esta opción si desea deshabilitar el cifrado de mensajes de correo electrónico.
  - **Utilizar TLS si es compatible con el servidor SMTP**

    Puede seleccionar esta opción si desea usar una conexión TLS con un servidor SMTP. Si el servidor SMTP no es compatible con TLS, el Servidor de administración se conecta con el servidor SMTP sin usar TLS.
  - **Utilizar siempre TLS, comprobar la validez del certificado del servidor**

    Puede seleccionar esta opción si desea usar la configuración de autenticación de TLS. Si el servidor SMTP no es compatible con TLS, el Servidor de administración no puede conectarse al servidor SMTP.

Le recomendamos que use esta opción para una mejor protección de la conexión con un servidor SMTP. Si selecciona esta opción, puede establecer la configuración de autenticación para una conexión TLS.

Si elige el valor **Always use TLS, check the server certificate for validity**, puede especificar un certificado para la autenticación del servidor SMTP y elegir si desea habilitar la comunicación a través de cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. También puede especificar un certificado para la autenticación de un cliente en el servidor SMTP.

Puede especificar la configuración de TLS para un servidor SMTP:

- Busque un archivo de certificados del servidor SMTP:

Puede recibir un archivo con la lista de certificados de una autoridad de certificación confiable y cargar el archivo al Servidor de administración. Kaspersky Security Center verifica si el certificado de un servidor SMTP también está firmado por una autoridad de certificación confiable. Si el certificado de un servidor SMTP no se recibe de una autoridad de certificación confiable, Kaspersky Security Center no podrá conectarse al servidor SMTP.

- Busque un archivo de certificados cliente:

Puede utilizar un certificado recibido de cualquier fuente (por ejemplo, de una entidad de certificación de confianza). Deberá especificar el certificado y su clave privada. Puede usar, para ello, alguno de los siguientes tipos de certificado:

- Certificado X-509:

Debe especificar un archivo con el certificado y un archivo con la clave privada. Estos dos archivos no dependen el uno del otro y el orden en que se los carga no es importante. Cuando se cargan ambos archivos, debe especificar la contraseña para decodificar la clave privada. Si la clave privada no está codificada, puede dejar la contraseña en blanco.

- contenedor pkcs12:

Debe cargar un solo archivo que contenga el certificado y la clave privada. Cuando se carga el archivo, debe especificar la contraseña para decodificar la clave privada. Si la clave privada no está codificada, puede dejar la contraseña en blanco.

El campo **Mensaje de notificación** contiene texto estándar con información sobre el evento que la aplicación envía cuando ocurre un evento. Este texto incluye parámetros sustitutos, como el nombre del evento, el nombre del dispositivo y el nombre del dominio. Puede editar el texto del mensaje agregando otros parámetros sustitutos con detalles más relevantes del evento. La lista de parámetros sustitutos está disponible haciendo clic en el botón a la derecha del campo.

Si el texto de la notificación contiene un signo de porcentaje (%), debe escribirlo dos veces seguidas para permitir el envío de mensajes. Por ejemplo: "La carga de la CPU es 100 %%".

Haga clic en el vínculo **Configurar el límite numérico de notificaciones** para especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

Haga clic en el botón **Enviar mensaje de prueba** para verificar si configuró las notificaciones correctamente. La aplicación debería enviar una notificación de prueba a las direcciones de correo electrónico que especificó.

- SMS

La pestaña **SMS** permite configurar la transmisión de notificaciones por SMS de diversos eventos a un teléfono celular. Los mensajes SMS se envían a través de una pasarela de correo.

En el campo **Destinatarios (direcciones de correo electrónico)**, especifique las direcciones de correo electrónico a las que la aplicación enviará notificaciones. Puede especificar varias direcciones en este campo, separándolas con punto y coma. Las notificaciones se enviarán a los números de teléfono asociados con las direcciones de correo electrónico especificadas.

En el campo **Servidores SMTP**, especifique las direcciones del servidor de correo, separándolas con punto y coma. Puede utilizar los siguientes parámetros:

- Dirección IPv4 o IPv6
- Nombre de la red de Windows (nombre NetBIOS) del dispositivo
- Nombre DNS del servidor SMTP

En el campo **Puerto del servidor SMTP**, especifique el número de un puerto de comunicación del servidor SMTP. El número de puerto predeterminado es 25.

Haga clic en el enlace **Configuración** para definir más ajustes de notificaciones:

- Nombre del sujeto (nombre del sujeto de un mensaje de correo electrónico)
- Dirección de correo electrónico del remitente
- Configuración de autenticación ESMTP

En caso de ser necesario, puede especificar una cuenta para autenticar en un servidor SMTP si la opción de autenticación de ESMTP está habilitada para un servidor SMTP.

- Configuración de TLS para un servidor SMTP

Puede deshabilitar el uso de TLS, usar TLS si el servidor SMTP admite este protocolo o forzar el uso de TLS únicamente. Si elige usar solo TLS, puede especificar un certificado para la autenticación del servidor SMTP y elegir si desea habilitar la comunicación a través de cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. Además, si elige usar solo TLS, puede especificar un certificado para la autenticación del cliente en el servidor SMTP.

- Busque un archivo de certificados del servidor SMTP

Puede recibir un archivo con la lista de certificados de una autoridad de certificación confiable y cargar el archivo a Kaspersky Security Center. Kaspersky Security Center verifica si el certificado del servidor SMTP también está firmado por una autoridad de certificación confiable. Si el certificado del servidor SMTP no se recibe de una autoridad de certificación confiable, Kaspersky Security Center no podrá conectarse al servidor SMTP.

Debe cargar un solo archivo que contenga el certificado y la clave privada. Cuando se carga el archivo, debe especificar la contraseña para decodificar la clave privada. La contraseña puede estar vacía si la clave privada no se encripta. El campo **Mensaje de notificación** contiene texto estándar con información sobre el evento que la aplicación envía cuando ocurre un evento. Este texto incluye parámetros sustitutos, como el nombre del evento, el nombre del dispositivo y el nombre del dominio. Puede editar el texto del mensaje agregando otros parámetros sustitutos con detalles más relevantes del evento. La lista de parámetros sustitutos está disponible haciendo clic en el botón a la derecha del campo.

Si el texto de la notificación contiene un signo de porcentaje (%), debe escribirlo dos veces seguidas para permitir el envío de mensajes. Por ejemplo: "La carga de la CPU es 100 %%".

Haga clic en el vínculo **Configurar límite numérico de notificaciones** para especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

Haga clic en el botón **Enviar mensaje de texto** para verificar si configuró las notificaciones correctamente. La aplicación debería enviar una notificación de prueba al destinatario que especificó.

- Archivo para ejecutar

  Si se selecciona este método de notificación, en el campo de entrada puede especificar la aplicación que se iniciará cuando ocurra un evento.

  Al hacer clic en el enlace **Configurar el límite numérico de notificaciones** podrá especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

  Al hacer clic en el botón **Enviar mensaje de prueba**, podrá verificar si configuró las notificaciones correctamente: la aplicación envía una notificación de prueba a las direcciones de correo electrónico que especificó.

5. En el campo **Mensaje de notificación**, escriba el texto que la aplicación enviará cuando se produzca un evento.

   Puede usar la lista desplegable a la derecha del campo de texto para agregar una configuración de sustitución con detalles del evento (por ejemplo, descripción del evento u hora en la que ocurre).

   Si el texto de la notificación contiene un porcentaje (%), lo debe especificar dos veces seguidas para permitir el envío del mensaje. Por ejemplo: "La carga de la CPU es 100 %%".

6. Haga clic en el botón **Enviar mensaje de prueba** para comprobar si la notificación se configuró correctamente.

   La aplicación envía una notificación de prueba al usuario especificado.

7. Haga clic en **Aceptar** para guardar los cambios.

Se implementa la configuración de notificación modificada en todos los eventos que ocurrieron en dispositivos cliente.

Puede anular la configuración de notificación para ciertos eventos en la sección **Configuración de eventos** de la configuración del Servidor de administración, de una configuración de directiva o de una configuración de aplicación.

## Creación de un certificado para un servidor SMTP

*Para crear un certificado para un servidor SMTP:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la pestaña **Eventos**.
3. Haga clic en el enlace **Configurar notificaciones y la exportación de eventos** y seleccione el valor **Configurar notificaciones** en la lista desplegable.

   Se abre la ventana de propiedades del evento.
4. En la pestaña **Correo electrónico**, haga clic en el enlace **Configuración** para abrir la ventana **Configuración**.
5. En la ventana **Configuración**, haga clic en el enlace **Especificar certificado** para abrir la ventana **Certificado para firmas**.
6. En la ventana **Certificado para firmas**, haga clic en el botón **Examinar**.

   Se abre la ventana **Certificado**.

7. En la lista desplegable **Tipo de certificado**, seleccione el tipo de certificado público o privado:

   - Si selecciona el tipo de certificado privado (**Contenedor PKCS #12**), especifique el archivo del certificado y la contraseña.

   - Si selecciona el tipo de certificado público (**Certificado X.509**):

     a. Especifique el archivo de clave privada (con las extensiones *.prk o *.pem).

     b. Especifique la contraseña de la clave privada.

     c. Especifique el archivo de clave pública (con la extensión *.cer).

8. Haga clic en **Aceptar**.

Se emite el certificado para el servidor SMTP.

# Selecciones de eventos

La información sobre los eventos del funcionamiento de Kaspersky Security Center y las aplicaciones administradas se guarda en la base de datos del Servidor de administración y en el registro del sistema de Microsoft Windows. Puede ver información de la base de datos del Servidor de administración en el espacio de trabajo del nodo **Servidor de administración**, en la pestaña **Eventos**.

La información de la pestaña **Eventos** se representa como una lista de selecciones de eventos. Cada selección incluye eventos de un tipo específico. Por ejemplo, la selección "El estado del dispositivo es Crítico" solo contiene registros de cambios de estado de dispositivos a "Crítico". Después de la instalación de la aplicación, la pestaña **Eventos** contiene algunas selecciones de eventos estándar. Puede crear selecciones adicionales (personalizadas) de eventos o exportar información de eventos a un archivo.

## Ver una selección de eventos

*Para ver una selección de eventos:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.

2. En el espacio de trabajo del nodo, abra la pestaña **Eventos**.

3. En la lista desplegable **Selecciones de eventos**, seleccione la selección de eventos correspondiente.

   Si desea que los eventos de esta selección se muestren constantemente en el espacio de trabajo, haga clic en el ícono de la estrella (☆) que se encuentra junto a la selección.

   El espacio de trabajo mostrará una lista de eventos, almacenados en el Servidor de administración, del tipo seleccionado.

Puede ordenar la información en la lista de eventos, en orden ascendente o descendente, en cualquier columna.

## Personalizar una selección de eventos

*Para personalizar una selección de eventos:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la pestaña **Eventos**.
3. Abra la selección de eventos correspondiente en la pestaña **Eventos**.
4. Haga clic en el botón **Propiedades de selección**.

En la ventana de propiedades de selección de eventos que se abre, puede configurar la selección de eventos.

## Crear una selección de eventos

*Para crear una selección de eventos:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la pestaña **Eventos**.
3. Haga clic en el botón **Crear selección**.
4. En la ventana **Nueva selección de eventos** que se abre, ingrese el nombre de la nueva selección y haga clic en **Aceptar**.

Se crea una selección con el nombre que especificó en la lista desplegable **Selecciones de eventos**.

De manera predeterminada, una selección de eventos creada contiene todos los eventos almacenados en el Servidor de administración. Para hacer que una selección solo muestre los eventos desea, debe personalizar la selección.

## Exportar una selección de eventos a un archivo de texto

*Para exportar una selección de eventos a un archivo de texto:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la pestaña **Eventos**.
3. Haga clic en el botón **Importar/Exportar**.
4. En la lista desplegable, seleccione **Exportar eventos a archivo**.

Se inicia el Asistente de exportación de eventos. Siga las instrucciones del asistente.

## Eliminar eventos de una selección

*Para eliminar eventos de la selección:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración correspondiente.
2. En el espacio de trabajo del nodo, abra la pestaña **Eventos**.
3. Seleccione los eventos que desea eliminar utilizando el ratón, la tecla **Mayús** o la tecla **Ctrl**.
4. Elimine los eventos seleccionados de una de las siguientes formas:
   - Seleccione **Eliminar** en el menú contextual de cualquiera de los eventos seleccionados.

     Si selecciona en el menú contextual el elemento **Eliminar todo**, se quitarán todos los eventos mostrados de la selección, sin tener en cuenta su selección de eventos para eliminar.
   - Haga clic en el enlace **Eliminar evento** si selecciona un evento, o bien en **Eliminar eventos** si selecciona varios eventos en la casilla de información para estos eventos.

Los eventos seleccionados se eliminan.

## Agregar aplicaciones a las exclusiones mediante solicitudes de los usuarios

Cuando recibe solicitudes de usuarios para desbloquear aplicaciones bloqueadas erróneamente, puede crear una exclusión de las reglas de seguridad adaptativa para estas aplicaciones. En consecuencia, las aplicaciones ya no serán bloqueadas en los dispositivos de los usuarios. Puede hacer un seguimiento del número de solicitudes de usuarios en la pestaña **Supervisión** del Servidor de administración.

*Para añadir aplicaciones bloqueadas por Kaspersky Endpoint Security a exclusiones por solicitudes de usuarios:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la pestaña **Eventos**.
3. En la lista desplegable **Selecciones de eventos**, seleccione **Solicitudes de usuario**.
4. Haga clic con el botón derecho en la solicitud del usuario (o en varias solicitudes del usuario) que contiene las aplicaciones que desea añadir a las exclusiones y luego seleccione **Agregar exclusión**.

   Esto inicia el Asistente para agregar exclusiones. Siga las instrucciones.

Las aplicaciones seleccionadas se excluirán de la lista de **Activación de reglas en el estado Aprendizaje inteligente** (ubicada dentro de **Repositorios** en el árbol de la consola) después de la próxima sincronización del dispositivo cliente con el Servidor de administración y ya no aparecerán en la lista.

# Selecciones de dispositivos

La información sobre el estado de los dispositivos se muestra en la carpeta **Selecciones de dispositivos** del árbol de consola.

La información de la carpeta **Selecciones de dispositivos** se muestra como una lista de selecciones de dispositivos. Cada selección contiene dispositivos que cumplen condiciones específicas. Por ejemplo, la selección **Dispositivos con estado Crítico** contiene únicamente dispositivos con el estado *Crítico*. Después de la instalación de la aplicación, la carpeta **Selecciones de dispositivos** contiene algunas selecciones estándar. Puede crear selecciones de dispositivos (personalizados) adicionales, exportar la configuración de la selección a un archivo o crear selecciones con la configuración importada desde otro archivo.

## Visualización de una selección de dispositivos

*Para ver una selección de dispositivos:*

1. En el árbol de la consola, seleccione la carpeta **Selecciones de dispositivos**.
2. En el espacio de trabajo de la carpeta, en la lista **Dispositivos en esta selección**, elija la selección de dispositivos que quiera ver.
3. Haga clic en el botón **Ejecutar selección**.
4. Haga clic en la pestaña **Resultados de la selección**.

El espacio de trabajo mostrará la lista de dispositivos que se ajustan a los criterios de la selección.

Puede ordenar la información de la lista de dispositivos tanto en orden ascendente como descendente, en cualquier columna.

## Configurar una selección de dispositivos

*Para configurar una selección de dispositivos:*

1. En el árbol de la consola, seleccione la carpeta **Selecciones de dispositivos**.
2. En el espacio de trabajo, haga clic en la pestaña **Selección**; a continuación, en la lista de selecciones de usuario, haga clic en la selección de dispositivos pertinente.
3. Haga clic en el botón **Propiedades de selección**.
4. En la ventana de propiedades que se abre, configure lo siguiente:
   - Propiedades de selección generales.
   - Las condiciones que se deben cumplir para dispositivos incluidos en esta selección. Para configurar las condiciones, deberá seleccionar el nombre de la condición y hacer clic en el botón **Propiedades**.
   - Los ajustes de seguridad.
5. Haga clic en **Aceptar**.

   El cambio se aplica y se guarda.

A continuación, se presentan descripciones de las condiciones para asignar dispositivos a una selección. Las condiciones se combinan usando el operador lógico OR: la selección incluirá dispositivos que cumplan con, al menos, una de las condiciones de la lista.

## General

En la sección **General**, puede cambiar el nombre de una condición de la selección y especificar si esa condición se debería invertir:

**Invertir condición de selección**

Esta opción está deshabilitada de forma predeterminada.

Si habilita esta opción, la condición elegida se aplicará a la inversa. La selección incluirá todos los dispositivos que no cumplan con la condición.

El siguiente ejemplo muestra la lógica del trabajo de inversión:

- **Condición**: en su dispositivo, hay un sistema operativo de tipo Linux y con número de compilación 00.0.000.
- **Condición invertida**: en su dispositivo, existe un sistema operativo con NOT (el tipo Linux y el número de compilación 00.0.000), lo que es equivalente a lo siguiente:

  Hay un sistema operativo con el tipo NOT Linux O el número de compilación NOT 00.0.000.

Por lo tanto, la selección incluirá los dispositivos con un sistema operativo, por ejemplo, del tipo Windows y el número de compilación 00.0.000, o del tipo Linux y cualquier número de compilación que no sea 00.0.000.

## Red

En la sección **Red**, puede especificar los criterios que serán usados para incluir dispositivos en la selección según sus datos de la red:

- **Nombre o dirección IP del dispositivo**

  Nombre de red de Windows (nombre NetBIOS) del dispositivo, o la dirección IPv4 o IPv6.

- **Dominio de Windows**

  Muestra todos los dispositivos incluidos en el dominio de Windows especificado.

- **Grupo de administración**

  Muestra los dispositivos incluidos en el grupo de administración especificado.

- **Descripción**

  Texto ubicado en el campo **Descripción** de la sección **General** dentro de la ventana de propiedades del dispositivo.

  Para describir el texto del campo **Descripción**, puede utilizar los siguientes caracteres:

  - Dentro de una palabra:

    - *****. Sustituye una cadena de cualquier largo (es decir, con cualquier número de caracteres).

    **Ejemplo**:

    Para describir palabras como **Servidor** o **Servidores**, puede ingresar **Servidor***.

    - **?.** Sustituye un carácter individual.

    **Ejemplo**:

    Para describir palabras como **Window** o **Windows**, puede ingresar **Windo?**.

    La consulta no puede comenzar con un asterisco (*****) ni con un signo de interrogación (**?**).

  - Para encontrar varias palabras:

    - Espacio. Muestra todos los dispositivos que tienen, en su descripción, alguna de las palabras indicadas.

    **Ejemplo**:

    Para encontrar una frase que contenga las palabras **secundario** o **virtual**, puede incluir la expresión **secundario virtual** en la consulta.

    - **+**. Si agrega el signo + antes de una palabra, todos los resultados de búsqueda contendrán esa palabra.

    **Ejemplo**:

    Para encontrar una frase que contenga las palabras **secundario** y **virtual**, ingrese la consulta **+secundario+virtual**.

    - **-**. Si agrega el signo - antes de una palabra, ningún resultado de búsqueda contendrá esa palabra.

    **Ejemplo**:

    Para encontrar una frase que contenga **secundario** y no contenga **virtual**, ingrese la consulta **+secundario-virtual**.

    - **"<cadena>"**. El texto que se ingresa entre comillas debe estar presente en el texto.

    **Ejemplo**:

    Para encontrar una frase que contenga la combinación de palabras **servidor secundario**, puede ingresar **"servidor secundario"** en la consulta.

- **Intervalo IP**

  Si habilita esta opción, podrá ingresar las direcciones IP inicial y final del intervalo IP en el que deberán estar incluidos los dispositivos pertinentes.

  Esta opción está deshabilitada de forma predeterminada.

## Etiquetas

En la sección **Etiquetas**, puede configurar criterios para dispositivos incluidos en una selección según palabras clave (etiquetas) que se agregaron anteriormente a las descripciones de dispositivos administrados:

- **Aplicar si coincide al menos una etiqueta especificada**

  Si habilita esta opción, los resultados de búsqueda mostrarán aquellos dispositivos que lleven, en su descripción, al menos una de las etiquetas seleccionadas.

  Si deshabilita esta opción, los resultados de búsqueda solo mostrarán aquellos dispositivos que no tengan ninguna de las etiquetas seleccionadas en su descripción.

  Esta opción está deshabilitada de forma predeterminada.

- **La etiqueta debe incluirse**

  Si selecciona esta opción, los resultados de búsqueda mostrarán aquellos dispositivos que lleven, en su descripción, la etiqueta seleccionada. La consulta de búsqueda puede incluir el asterisco, que representa una cadena de cualquier longitud (número de caracteres).

  Esta opción está seleccionada de manera predeterminada.

- **La etiqueta debe excluirse**

  Si selecciona esta opción, los resultados de búsqueda mostrarán aquellos dispositivos que no lleven en su descripción la etiqueta seleccionada. La consulta de búsqueda puede incluir el asterisco, que representa una cadena de cualquier longitud (número de caracteres).

## Active Directory

En la sección **Active Directory**, puede configurar criterios para dispositivos incluidos en una selección según sus datos de Active Directory:

- **El dispositivo está en una unidad organizativa de Active Directory**

  Si habilita esta opción, la selección incluirá los dispositivos de la unidad organizativa de Active Directory especificada en el campo de entrada.

  Esta opción está deshabilitada de forma predeterminada.

- **Incluir unidades de organización secundarias**

  Si habilita esta opción, la selección incluirá los dispositivos de todas las unidades organizativas secundarias de la unidad organizativa del dominio especificado.

  Esta opción está deshabilitada de forma predeterminada.

- **El dispositivo es miembro de un grupo de Active Directory**

  Si habilita esta opción, la selección incluirá los dispositivos que pertenezcan al grupo de Active Directory especificado en el campo de entrada.

  Esta opción está deshabilitada de forma predeterminada.

## Actividad de red

En la sección **Actividad de red**, puede establecer los criterios que se usarán para incluir dispositivos en la selección basándose en la actividad de red de los mismos:

- El dispositivo es un punto de distribución

  En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

  - **Sí**. La selección incluirá dispositivos que funcionen como punto de distribución.
  - **No**. La selección no incluirá dispositivos que funcionen como punto de distribución.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

- No desconectar del Servidor de administración

  En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

  - **Habilitado**. La selección incluirá dispositivos en los que esté activada la casilla **No desconectar del Servidor de administración**.
  - **Deshabilitado**. La selección incluirá dispositivos en los que no esté activada la casilla **No desconectar del Servidor de administración**.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

- Perfil de conexión cambiado

  En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

  - **Sí**. La selección incluirá dispositivos que se hayan conectado al Servidor de administración tras un cambio de perfil de conexión.
  - **No**. La selección no incluirá dispositivos que se hayan conectado al Servidor de administración tras un cambio de perfil de conexión.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

- Última conexión con el Servidor de administración

  Puede utilizar esta casilla para establecer un criterio de búsqueda de dispositivos que se base en el momento en el que haya ocurrido la última conexión al Servidor de administración.

  Si activa esta casilla, podrá usar los campos de entrada para indicar el intervalo de tiempo (fecha y hora) en el que deberá haber ocurrido la última conexión entre el Agente de red instalado en el dispositivo cliente y el Servidor de administración. La selección incluirá aquellos dispositivos que estén alcanzados por el intervalo especificado.

  Si no activa esta casilla, no se aplicará este criterio.

  Esta casilla no está marcada de manera predeterminada.

- Nuevos dispositivos detectados por sondeo de red

  Utilice esta opción para buscar dispositivos nuevos, que se hayan detectado durante los sondeos de red realizados en días recientes.

  Si habilita esta opción, la selección incluirá solo aquellos dispositivos nuevos que se hayan detectado mediante el descubrimiento de dispositivos en el intervalo de días especificado en el campo **Periodo de detección (días)**.

  Si deshabilita esta opción, la selección incluirá todos los dispositivos detectados por el mecanismo de descubrimiento.

  Esta opción está deshabilitada de forma predeterminada.

- Dispositivo visible

  En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

  - **Sí**. La selección incluirá aquellos dispositivos que sean visibles en la red.
  - **No**. La selección incluirá aquellos dispositivos que no sean visibles en la red.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

## Aplicación

En la sección **Aplicación**, puede configurar criterios para incluir dispositivos en una selección según la aplicación administrada seleccionada:

- Nombre de la aplicación

  En la lista desplegable, puede definir un criterio para incluir dispositivos en la selección cuando se realice una basada en el nombre de una aplicación de Kaspersky.

  La lista solo contendrá los nombres de aquellas aplicaciones que tengan su respectivo complemento de administración instalado en la estación de trabajo del administrador.

  Si no selecciona ninguna aplicación, este criterio no se aplicará.

- Versión de la aplicación

  En el campo de entrada, puede definir un criterio para incluir dispositivos en la selección cuando se realice una búsqueda basada en el número de versión de una aplicación de Kaspersky.

  Si no especifica un número de versión, este criterio no se aplicará.

- Nombre de la actualización crítica

  En el campo de entrada, puede definir un criterio para incluir dispositivos en la selección cuando se realice una búsqueda basada en el nombre de una aplicación o en un número de paquete de actualización.

  Si el campo queda en blanco, este criterio no se aplicará.

- Última actualización de módulos

  Use esta opción para definir un criterio que permita buscar dispositivos según la hora en que se hayan actualizado por última vez los módulos de las aplicaciones instaladas en ellos.

  Si activa esta casilla, podrá utilizar los campos de entrada para definir el intervalo de tiempo (fecha y hora) en el que deberá haber ocurrido la última actualización de módulos de las aplicaciones instaladas en los dispositivos.

  Si no activa esta casilla, no se aplicará este criterio.

  Esta casilla no está marcada de manera predeterminada.

- El dispositivo se administra a través de Kaspersky Security Center

  Puede usar la lista desplegable para que la selección incluya aquellos dispositivos que se administren mediante Kaspersky Security Center:

  - **Sí**. La selección incluirá aquellos dispositivos que se administren mediante Kaspersky Security Center.
  - **No**. La aplicación incluirá aquellos dispositivos que no se administran mediante Kaspersky Security Center Linux.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

- La aplicación de seguridad está instalada

  Puede usar la lista desplegable para que la selección incluya aquellos dispositivos que tengan instalada la aplicación de seguridad:

  - **Sí**. La selección incluirá aquellos dispositivos en los que se haya instalado la aplicación de seguridad.
  - **No**. La selección incluirá aquellos dispositivos en los que no se haya instalado la aplicación de seguridad.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

## Sistema operativo

En la sección **Sistema operativo**, puede especificar los criterios que serán usados para incluir dispositivos en la selección según el tipo de sistema operativo.

- Versión del sistema operativo

  Si activa esta casilla, podrá seleccionar un sistema operativo de la lista. Los dispositivos que tengan instalado ese sistema operativo se incluirán en los resultados de búsqueda.

- Arquitectura del sistema operativo

  En la lista desplegable, puede seleccionar la arquitectura para la que deberá estar diseñado el sistema operativo. Los valores posibles son **Desconocido**, **x86**, **AMD64** e **IA64**. La arquitectura que elija determinará el modo de aplicar la regla de movimiento al dispositivo. De manera predeterminada, no hay ninguna opción seleccionada en la lista (es decir, la arquitectura del sistema operativo no está definida).

- Versión de Service Pack del sistema operativo

  En este campo, puede especificar la versión del paquete de su sistema operativo (en formato *X.Y*), que determinará cómo aplicar la regla de migración a su dispositivo. De manera predeterminada, no hay una versión definida.

- Compilación del sistema operativo

  Este parámetro solo es válido para sistemas operativos Windows.

  Número de compilación del sistema operativo. Puede indicar si el número de compilación del sistema operativo seleccionado deberá ser igual, anterior o posterior al valor introducido. También puede hacer que la búsqueda incluya todos los números de compilación, excepto el especificado.

- Id. de versión del sistema operativo

  Este parámetro solo es válido para sistemas operativos Windows.

  Identificador de versión del sistema operativo. Puede indicar si el sistema operativo seleccionado deberá tener un id. de versión igual, anterior o posterior al valor introducido. También puede hacer que la búsqueda incluya todos los id. de versión, excepto el especificado.

## Estado del dispositivo

En la sección **Estado del dispositivo**, puede configurar criterios para incluir dispositivos en una selección según la descripción del estado de dispositivos de una aplicación administrada:

- Estado del dispositivo

  Lista desplegable en la que puede seleccionar un estado de dispositivo: *Sin inconvenientes*, *Crítico* o *Advertencia*.

- Descripción del estado del dispositivo

  En este campo, puede activar casillas correspondientes a condiciones que, al cumplirse, hacen que el dispositivo tome uno de los siguientes estados: *Sin inconvenientes, Crítico* o *Advertencia*.

- Estado del dispositivo definido por la aplicación

  Lista desplegable en la cual puede seleccionar el estado de la protección en tiempo real. La selección incluirá aquellos dispositivos que tengan el estado de protección en tiempo real indicado.

## Componentes de protección

En la sección **Componentes de protección**, puede configurar los criterios para incluir dispositivos en una selección en función de su estado de protección:

- **Bases de datos publicadas**

  Seleccione esta opción para buscar dispositivos cliente basándose en la fecha de publicación de las bases de datos antivirus. Utilice el campo de entrada para definir el intervalo de tiempo que se tomará como base para la búsqueda.

  Esta opción está deshabilitada de forma predeterminada.

- **Último análisis**

  Habilite esta opción para buscar dispositivos cliente basándose en la hora del último análisis antimalware. Utilice los campos de entrada para definir el período en el cual deberá haber ocurrido el último análisis antimalware.

  Esta opción está deshabilitada de forma predeterminada.

- **Número total de amenazas detectadas**

  Habilite esta opción para buscar dispositivos cliente basándose en el número de virus detectados. Utilice los campos de entrada para definir los valores que se tomarán como umbral superior e inferior del número de virus detectados.

  Esta opción está deshabilitada de forma predeterminada.

## Registro de aplicaciones

En la sección **Registro de aplicaciones**, puede configurar los criterios para buscar dispositivos según las aplicaciones que tienen instaladas:

- **Nombre de la aplicación**

  Lista desplegable en la que puede seleccionar una aplicación. Los dispositivos que tengan instalada la aplicación elegida se incluirán en la selección.

- **Versión de la aplicación**

  Campo de entrada en el que puede especificar la versión de la aplicación seleccionada.

- **Proveedor**

  Lista desplegable en la que puede seleccionar el desarrollador de una aplicación instalada en el dispositivo.

- **Estado de la aplicación**

  Lista desplegable en la que puede seleccionar el estado de la aplicación (*Instalada*, *Sin instalar*). Se incluirán en la selección los dispositivos que tengan o no tengan (dependiendo del estado seleccionado) la aplicación seleccionada.

- **Buscar por actualización**

  Si habilita esta opción, la búsqueda se basará en los detalles de las actualizaciones para el software instalado en los dispositivos pertinentes. Una vez que active esta casilla, los campos **Nombre de la aplicación**, **Versión de la aplicación** y **Estado de la aplicación** cambiarán a **Nombre de actualización**, **Versión de actualización** y **Estado**, respectivamente.

  Esta opción está deshabilitada de forma predeterminada.

- **Nombre de la aplicación de seguridad incompatible**

  Lista desplegable en la que puede seleccionar aplicaciones de seguridad de terceros. Los dispositivos que tengan instalada la aplicación seleccionada serán incluidos en la selección cuando se realice la búsqueda.

- **Etiqueta de aplicación**

  Lista desplegable en la que puede seleccionar una etiqueta de aplicación. Se incluirán en la selección aquellos dispositivos que tengan instaladas aplicaciones que, en su descripción, contengan la etiqueta seleccionada.

- **Aplicar a los dispositivos que no tengan las etiquetas especificadas**

  Si habilita esta opción, la selección incluirá aquellos dispositivos que no contengan ninguna de las etiquetas seleccionadas en su descripción.

  Si deshabilita esta opción, no se aplicará el criterio.

  Esta opción está deshabilitada de forma predeterminada.

## Registro de hardware

En la sección **Registro de hardware**, puede configurar criterios para incluir dispositivos en la selección basándose en el hardware que tengan instalado:

- **Dispositivo**

  En la lista desplegable, puede seleccionar un tipo de unidad. Los dispositivos que tengan la unidad seleccionada se incluirán en los resultados de búsqueda.

  El campo permite realizar búsquedas de texto completo.

- **Proveedor**

  En la lista desplegable, puede seleccionar el nombre del fabricante de la unidad. Los dispositivos que tengan la unidad seleccionada se incluirán en los resultados de búsqueda.

  El campo permite realizar búsquedas de texto completo.

- **Nombre del dispositivo**

  Nombre del dispositivo en la red de Windows. El dispositivo con el nombre especificado se incluirá en la selección.

- **Descripción**

  Descripción del dispositivo o unidad de hardware. Los dispositivos que tengan la descripción indicada en este campo se incluirán en la selección.

  Si desea agregar una descripción a un dispositivo, puede hacerlo (en cualquier formato) a través de la ventana de propiedades del mismo. El campo permite realizar búsquedas de texto completo.

- **Proveedor del dispositivo**

  Nombre del fabricante del dispositivo. Los dispositivos producidos por el fabricante especificado en este campo se incluyen en la selección.

  Puede ingresar el nombre del fabricante en la ventana de propiedades de un dispositivo.

- **Número de serie**

  Todas las unidades de hardware con el número de serie especificado en este campo se incluirán en la selección.

- **Número de inventario**

  Los equipos que tengan el número de inventario indicado en este campo se incluirán en la selección.

- **Usuario**

  Todas las unidades de hardware del usuario especificado en este campo se incluirán en la selección.

- **Ubicación**

  Ubicación de un dispositivo o una unidad de hardware (por ejemplo, en la sede central o en una sucursal). Las computadoras o dispositivos que se encuentren en la ubicación especificada en este campo se incluirán en la selección.

  Puede describir la ubicación de un dispositivo en cualquier formato en la ventana de propiedades de dicho dispositivo.

- **Frecuencia de la CPU, en MHz**

  Intervalo de frecuencias de un procesador. La selección incluirá aquellos dispositivos que tengan un procesador con un intervalo de frecuencias comprendido en los límites dispuestos en los campos (inclusive).

- **Núcleos de CPU virtuales**

  Intervalo del número de núcleos virtuales de un procesador. La selección incluirá aquellos dispositivos que tengan un procesador comprendido en los límites dispuestos en los campos (inclusive).

- **Volumen de disco duro, en GB**

  Intervalo de valores referentes al tamaño del disco duro instalado en el dispositivo. La selección incluirá aquellos dispositivos que tengan un disco duro comprendido en los límites dispuestos en los campos (inclusive).

- **Tamaño de RAM, en MB**

  Rango de valores para el tamaño de la memoria RAM del dispositivo. Los dispositivos cuya memoria RAM coincida con los intervalos de estos campos de entrada (inclusive) se incluirán en la selección.

## Máquinas virtuales

En la sección **Máquinas virtuales**, puede configurar los criterios que se usarán para incluir dispositivos en la selección basándose en el hecho de que sean máquinas virtuales o de que formen parte de una infraestructura de escritorios virtuales (VDI):

- **Es una máquina virtual**

  En la lista desplegable puede seleccionar las siguientes opciones:

  - **No es importante**.
  - **No**. Buscar dispositivos que no sean máquinas virtuales.
  - **Sí**. Buscar dispositivos que sean máquinas virtuales.

- **Tipo de máquina virtual**

  En la lista desplegable, puede seleccionar el desarrollador de la máquina virtual.

  Esta lista desplegable estará disponible si seleccionó los valores **Sí** o **No es importante** en la lista desplegable **Es una máquina virtual**.

- **Parte de la infraestructura de escritorio virtual**

  En la lista desplegable puede seleccionar las siguientes opciones:

  - **No es importante**.
  - **No**. Buscar dispositivos que no sean parte de la Infraestructura de escritorio virtual.
  - **Sí**. Buscar dispositivos que sean parte de una VDI.

## Vulnerabilidades y actualizaciones

En la sección **Vulnerabilidades y actualizaciones**, puede especificar los criterios que se usarán para incluir dispositivos en la selección basándose en el origen de Windows Update que utilicen:

**WUA está ahora conectado al Servidor de administración**

En la lista desplegable, puede seleccionar una de las siguientes opciones de búsqueda:

- **Sí**. Si selecciona esta opción, los resultados de búsqueda incluirán aquellos dispositivos que reciban sus actualizaciones de Windows Update del Servidor de administración.
- **No**. Si selecciona esta opción, los resultados incluirán aquellos dispositivos que reciban sus actualizaciones de Windows Update de cualquier otro origen.

## Usuarios

En la sección **Usuarios**, puede configurar los criterios para incluir dispositivos en la selección basándose en las cuentas de usuario con las que se haya iniciado sesión en el sistema operativo.

- **Último usuario que inició sesión en el sistema**

  Si habilita esta opción, podrá hacer clic en el botón **Examinar** para seleccionar una cuenta de usuario. Los resultados de búsqueda incluirán aquellos dispositivos en los que el usuario indicado haya sido el último en iniciar sesión.

- **Usuario que inició sesión en el sistema al menos una vez**

  Si habilita esta opción, podrá hacer clic en el botón **Examinar** para seleccionar una cuenta de usuario. Los resultados de búsqueda incluirán aquellos dispositivos en los que el usuario indicado haya iniciado sesión al menos una vez.

## Problemas que afectan al estado en las aplicaciones administradas

En la sección **Problemas que afectan al estado en las aplicaciones administradas**, puede especificar los criterios que se utilizarán para incluir dispositivos en la selección de acuerdo con la lista de posibles problemas detectados por una aplicación administrada. Si un dispositivo tiene al menos uno de los problemas elegidos, ese dispositivo se incluirá en la selección. Cuando selecciona un problema listado para varias aplicaciones, tiene la opción de seleccionar este problema en todas las listas automáticamente.

**Descripción del estado del dispositivo**

Puede activar casillas correspondientes a las descripciones de estado reportadas por la aplicación administrada. Cuando se reciban esos estados, los dispositivos correspondientes se incluirán en la selección. Si elige un estado incluido en las listas de varias aplicaciones, tendrá la opción de seleccionar todos los casos automáticamente.

## Estados de componentes en aplicaciones administradas

En la sección **Estados de componentes en aplicaciones administradas**, puede configurar los criterios que se usarán para incluir dispositivos en la selección basándose en los estados de los componentes de las aplicaciones administradas:

- **Estado de Prevención de fugas de datos**

  Buscar dispositivos basándose en el estado de Prevención de fuga de datos (*Desconocido, Detenida, Iniciándose, En pausa, En ejecución, Error*).

- **Estado de protección de los servidores de colaboración**

  Buscar dispositivos basándose en el estado de la protección para servidores de colaboración (*Desconocido*, *Detenida*, *Iniciándose, En pausa*, *En ejecución*, *Error*).

- **Estado de protección antivirus en servidores de correo**

  Buscar dispositivos basándose en el estado de la protección para servidores de correo (*Desconocido, Detenida, Iniciándose, En pausa, En ejecución, Error).*

- **Estado de Sensor de Endpoint**

  Buscar dispositivos basándose en el estado del componente Sensor de Endpoint (*Desconocido, Detenida, Iniciándose, En pausa, En ejecución, Error*).

## Cifrado

**Algoritmo de cifrado**

Algoritmo de cifrado de bloque simétrico AES. En la lista desplegable, puede seleccionar el tamaño de la clave de cifrado (56 bits, 128 bits, 192 bits o 256 bits).

Valores disponibles: *AES56*, *AES128*, *AES192* y *AES256*.

## Segmentos de nube

En la sección **Segmentos de nube**, puede configurar criterios para incluir dispositivos en la selección basándose en los segmentos de nube vinculados a esos dispositivos:

- **El dispositivo se encuentra en un segmento de nube**

  Si habilita esta opción, podrá hacer clic en el botón **Examinar** para seleccionar el segmento de búsqueda.

  Si también habilita la opción **Incluir objetos secundarios**, la búsqueda se realizará en todos los objetos secundarios del segmento elegido.

  Los resultados de la búsqueda solo incluirán aquellos dispositivos que estén en el segmento seleccionado.

- **Dispositivo encontrado mediante API**

  La lista desplegable le permite operar con el hecho de que el dispositivo pueda detectarse con las herramientas provistas por una API.

  - **AWS**. El dispositivo se descubre mediante la API de AWS, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de AWS.
  - **Azure**. El dispositivo se descubre mediante la API de Azure, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de Azure.
  - **Google Cloud.** El dispositivo se descubre utilizando la API de Google, es decir, el dispositivo está en el entorno de Google Cloud.
  - **No**. El dispositivo no se puede detectar con la API de AWS, Azure o Google (o bien el dispositivo no se encuentra en el entorno de nube, o bien sí está en el entorno de nube, pero, por algún motivo, no se lo puede detectar con una API).
  - **Ningún valor.** Esta condición no se aplica.

## Componentes de las aplicaciones

En esta sección, se enumeran los componentes de aquellas aplicaciones que tienen instalado un complemento de administración en la Consola de administración.

En la sección **Componentes de las aplicaciones**, puede definir criterios para incluir dispositivos en la selección basándose en los estados y los números de versión de los componentes vinculados a una aplicación seleccionada:

- **Estado**

  Buscar dispositivos basándose en el estado de un componente reportado por una aplicación al Servidor de administración. Puede seleccionar uno de los siguientes estados: *No hay datos del dispositivo*, *Detenido*, *Iniciándose*, *En pausa*, *En ejecución*, *Error de funcionamiento* y *Sin instalar*. Si el componente seleccionado de la aplicación instalada en un dispositivo administrado tiene el estado especificado, el dispositivo será incluido en la selección de dispositivos.

  Estados reportados por las aplicaciones:

  - *Iniciándose*: el componente está en proceso de iniciarse.
  - *En ejecución*: el componente está habilitado y funciona correctamente.
  - *En pausa*: el componente se encuentra suspendido (por ejemplo, porque el usuario pausó la protección en la aplicación administrada).
  - *Error de funcionamiento*: ocurrió un error durante el funcionamiento del componente.
  - *Detenido*: el componente está deshabilitado y no se encuentra en funcionamiento.
  - *Sin instalar*: el usuario no optó por instalar el componente al realizar una instalación personalizada de la aplicación.

  A diferencia de los demás estados, *No hay datos del dispositivo* no es un estado reportado por las aplicaciones. Se trata de una opción que muestra que las aplicaciones no tienen información sobre el estado del componente seleccionado. Esta situación puede presentarse, por ejemplo, cuando el componente seleccionado no pertenece a ninguna de las aplicaciones instaladas en el dispositivo o cuando el dispositivo está apagado.

- **Versión**

  Buscar dispositivos basándose en el número de versión del componente seleccionado en la lista. Puede escribir un número de versión, por ejemplo `3.4.1.0`, y luego especificar si el componente seleccionado debe tener una versión igual, anterior o posterior. También puede configurar la búsqueda de todas las versiones excepto la especificada.

## Exportar la configuración de una selección de dispositivos a un archivo

*Para exportar las configuraciones de una selección de dispositivos a un archivo de texto:*

1. En el árbol de la consola, seleccione la carpeta **Selecciones de dispositivos**.
2. En el espacio de trabajo, haga clic en la pestaña **Selección** y luego, en la lista de selecciones de usuario, haga clic en la selección de dispositivos que le interese.

   Únicamente podrá exportar la configuración de selecciones que hayan sido creadas por un usuario.

3. Haga clic en el botón **Ejecutar selección**.

4. En la pestaña **Resultados de la selección**, haga clic en el botón **Exportar configuración**.

5. En la ventana **Guardar como** que se abre, especifique un nombre para el archivo de exportación de la configuración de selección, seleccione una carpeta para guardarlo y haga clic en el botón **Guardar**.

La configuración de la selección de dispositivos se guardará en el archivo especificado.

## Crear una selección de dispositivos

*Para crear una selección de dispositivos:*

1. En el árbol de la consola, seleccione la carpeta **Selecciones de dispositivos**.

2. En el espacio de trabajo de la carpeta, haga clic en **Avanzado** y seleccione **Crear selección** en la lista desplegable.

3. En la ventana **Nueva selección de dispositivos** que se abre, ingrese el nombre de la nueva selección y haga clic en **Aceptar**.

Aparecerá una nueva carpeta con el nombre que ingresó en la carpeta **Selecciones de dispositivos** del árbol de consola. De manera predeterminada, la nueva selección de dispositivos contiene todos los dispositivos incluidos en los grupos de administración del Servidor de administración en el que se creó la selección. Para que una selección muestre solo los dispositivos que le interesan, configure la selección haciendo clic en el botón **Propiedades de selección**.

## Crear una selección de dispositivos según la configuración importada

*Crear una selección de dispositivos según una configuración importada*

1. En el árbol de la consola, seleccione la carpeta **Selecciones de dispositivos**.

2. En el espacio de trabajo de la carpeta, haga clic en el botón **Avanzado** y seleccione **Importar selección desde archivo** en la lista desplegable.

3. En la ventana que se abre, especifique la ruta del archivo desde el cual desea importar las configuraciones de selección. Haga clic en el botón **Abrir**.

Una entrada **Nueva selección** se crea en la carpeta **Selecciones de dispositivos**. La configuración de la selección nueva se importa del archivo que especificó.

Si ya existe una selección llamada **Nueva selección** en la carpeta **Selecciones de dispositivos**, se agrega un índice en formato **(<siguiente número de la secuencia>)** al nombre de la selección creada, por ejemplo: **(1)**, **(2)**.

## Eliminación de dispositivos de los grupos de administración en una selección

Cuando se trabaja con la selección de dispositivos, puede eliminar los dispositivos de los grupos de administración en la misma selección, sin cambiar a los grupos de administración de los que se deben eliminar estos dispositivos.

*Para eliminar los dispositivos de los grupos de administración:*

1. En el árbol de la consola, seleccione la carpeta **Selecciones de dispositivos**.
2. Seleccione los dispositivos que quiera quitar mediante las teclas **Mayús** o **Ctrl**.
3. Quite los dispositivos seleccionados de los grupos de administración por alguno de los medios siguientes:
   - Seleccione **Eliminar** en el menú contextual de cualquiera de los dispositivos seleccionados.
   - Haga clic en el botón **Realizar acción** y seleccione **Eliminar del grupo** en la lista desplegable.

Los dispositivos seleccionados se quitarán de los grupos de administración correspondientes.

# Supervisión de instalación y desinstalación de aplicaciones

Puede supervisar la instalación y desinstalación de aplicaciones específicas en dispositivos administrados (por ejemplo, un navegador específico). Para usar esta función, puede agregar aplicaciones del Registro de aplicaciones a la lista de aplicaciones supervisadas. Cuando se instala o desinstala una aplicación supervisada, el Agente de red publica los eventos respectivos: **Se instaló una aplicación supervisada** o **Se desinstaló una aplicación supervisada**. Puede supervisar estos eventos utilizando, por ejemplo, selecciones de eventos o informes.

Puede supervisar estos eventos solo si están almacenados en la base de datos del Servidor de administración.

*Para agregar una aplicación a la lista de aplicaciones supervisadas:*

1. En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Registro de aplicaciones**.
2. Encima de la lista de aplicaciones que se muestra, haga clic en el botón **Mostrar ventana de propiedades del registro de aplicaciones**.
3. En la ventana **Aplicaciones supervisadas** que se muestra, haga clic en el botón **Agregar**.
4. En la ventana que se muestra **Seleccione el nombre de la aplicación**, seleccione las aplicaciones del Registro de aplicaciones cuya instalación o desinstalación desea supervisar.
5. En la ventana **Seleccione el nombre de la aplicación**, haga clic en el botón **Aceptar**.

Después de configurar la lista de aplicaciones supervisadas y de que una aplicación supervisada se instale o desinstale en los dispositivos administrados en su organización, puede supervisar los eventos respectivos, por ejemplo, al utilizar la selección de eventos Eventos recientes.

# Eventos de los componentes de Kaspersky Security Center

Cada componente de Kaspersky Security Center tiene su propio conjunto de tipos de evento. En esta sección, se enumeran los tipos de eventos que ocurren en el Servidor de administración de Kaspersky Security Center, el Agente de red y el Servidor de MDM para iOS. Los tipos de eventos que pueden ocurrir en las aplicaciones de Kaspersky no se detallan en esta sección.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Para el Servidor de administración, también puede ver y configurar la lista de eventos en las propiedades del Servidor de administración. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

## Estructura de datos utilizada para describir los tipos de eventos

Cada tipo de evento tiene especificado su nombre, identificador (id.), código alfabético, descripción y plazo de almacenamiento predeterminado.

- **Nombre que se muestra para el tipo de evento**. Este texto se muestra en Kaspersky Security Center cuando configura los eventos y cuando ocurren.
- **Id. del tipo de evento**. Un código numérico que se utiliza para procesar los eventos con una herramienta de análisis de eventos desarrollada por un tercero.
- **Tipo de evento** (código alfabético). Este código se usa cuando navega y procesa eventos utilizando vistas públicas que se proporcionan en la base de datos de Kaspersky Security Center y cuando los eventos se exportan a un sistema SIEM.
- **Descripción**. Un texto en el que se describen las situaciones en las que ocurren un evento y las acciones que se pueden tomar en cada caso.
- **Plazo de almacenamiento predeterminado**. El número de días por los que cada evento queda almacenado en la base de datos del Servidor de administración. Este es, también, el tiempo por el que el evento aparece en la lista de eventos del Servidor de administración. Transcurrido este período, el evento se elimina. Cuando el plazo de almacenamiento es 0, el evento se detecta, pero no se lo muestra en la lista de eventos del Servidor de administración. Si se configuró para guardar dichos eventos en el registro de eventos del sistema operativo, puede encontrarlos allí.

  Puede cambiar el plazo de almacenamiento para eventos:

  - Consola de administración: Configuración del plazo de almacenamiento para un evento
  - Kaspersky Security Center Web Console: Configuración del plazo de almacenamiento para un evento

Otros datos pueden incluir los siguientes campos:

- **event_id**: número único del evento en la base de datos, generado y asignado automáticamente; no se debe confundir con el **ID del tipo de evento**.
- **task_id**: el ID de la tarea que causó el evento (si lo hay).
- **gravedad**: uno de los siguientes niveles de gravedad (en orden ascendente de gravedad):

  0) Nivel de gravedad no válido

  1) Info.

  2) Advertencia

  3) Error

  4) Crítico

# Eventos del Servidor de administración

En esta sección, se brinda información sobre los eventos relacionados con el Servidor de administración.

## Eventos del Servidor de administración: nivel Crítico

En la siguiente tabla, se enumeran los tipos de eventos del Servidor de administración de Kaspersky Security Center que tienen el nivel de importancia **Crítico**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Para el Servidor de administración, también puede ver y configurar la lista de eventos en las propiedades del Servidor de administración. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Si especificó el puerto en la ventana de propiedades del Servidor de administración en la Consola de administración, **Kaspersky Security Center publica las métricas** y los eventos críticos que debe obtener Prometheus, un sistema de supervisión y alerta. Prometheus obtiene las métricas y los eventos críticos y, luego, genera alertas para cada evento.

// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Se ha superado el límite de la licencia** | 4099 | KLSRV_EV_LICENSE_CHECK_MORE_110 | Una vez al día, Kaspersky Security Center comprueba si se superó algún límite de licencia.<br>Este tipo de evento ocurre cuando el Servidor de administración detecta que las aplicaciones de Kaspersky instaladas en los dispositivos cliente han superado algún límite de sus licencias y se ha utilizado más de un 110 % del total de unidades con licencia cubiertas por una sola licencia.<br>Los dispositivos cliente se mantienen protegidos aun cuando ocurre este evento.<br>Puede responder al evento de los siguientes modos:<br>• Revise la lista de dispositivos administrados. Elimine los dispositivos que no estén en uso.<br>• Agregue una licencia para más dispositivos (agregue un código de activación válido o un archivo de clave en el Servidor de administración).<br>Kaspersky Security Center determina las reglas para generar eventos cuando se supera un límite de licencia. | 180 días |
| **Brote de virus** | 26 (para Protección contra archivos peligrosos) | GNRL_EV_VIRUS_OUTBREAK | Los eventos de este tipo ocurren cuando el número de objetos maliciosos detectados en varios dispositivos administrados supera el umbral en un corto período de tiempo.<br>Puede responder al evento de los siguientes modos:<br>• Configure el umbral en las propiedades del Servidor de administración.<br>• Cree una directiva más estricta que se active cuando ocurra este evento (o, como alternativa, cree una tarea que se ejecute cuando ocurra el evento). | 180 días |
| **Brote de virus** | 27 (para Protección contra amenazas de correo) | GNRL_EV_VIRUS_OUTBREAK | Los eventos de este tipo ocurren cuando el número de objetos maliciosos detectados en varios dispositivos administrados supera el umbral en un corto período de tiempo.<br>Puede responder al evento de los siguientes modos:<br>• Configure el umbral en las propiedades del Servidor de administración.<br>• Cree una directiva más estricta que se active cuando ocurra este evento (o, como alternativa, cree una tarea que se ejecute cuando ocurra el evento). | 180 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Brote de virus** | 28 (para el firewall) | GNRL_EV_VIRUS_OUTBREAK | Los eventos de este tipo ocurren cuando el número de objetos maliciosos detectados en varios dispositivos administrados supera el umbral en un corto período de tiempo.<br>Puede responder al evento de los siguientes modos:<br>• Configure el umbral en las propiedades del Servidor de administración.<br>• Cree una directiva más estricta que se active cuando ocurra este evento (o, como alternativa, cree una tarea que se ejecute cuando ocurra el evento). | 180 días |
| **El dispositivo ha cambiado a no administrado** | 4111 | KLSRV_HOST_OUT_CONTROL | Este tipo de eventos ocurren si un dispositivo administrado es visible en la red pero no se ha conectado al Servidor de administración durante un período específico.<br>Averigüe qué impide el correcto funcionamiento del Agente de red en el dispositivo. El problema podría deberse a un inconveniente en la red, por ejemplo, o al hecho de que el Agente de red se haya eliminado del dispositivo. | 180 días |
| **El estado del dispositivo es Crítico** | 4113 | KLSRV_HOST_STATUS_CRITICAL | Este tipo de evento ocurre cuando se le asigna el estado *Crítico* a un dispositivo administrado. Puede configurar las condiciones bajo las cuales el estado del dispositivo se cambia a *Crítico*. | 180 días |
| **El archivo de clave está en la lista de claves rechazadas** | 4124 | KLSRV_LICENSE_BLACKLISTED | Este tipo de evento ocurre cuando Kaspersky ha agregado el código de activación o el archivo de clave utilizados a la lista de rechazados.<br>Comuníquese con nuestro servicio de soporte técnico para más información. | 180 días |
| **Modo de funcionalidad limitada** | 4130 | KLSRV_EV_LICENSE_SRV_LIMITED_MODE | Este tipo de evento ocurre cuando Kaspersky Security Center pasa a operar con sus funciones básicas, sin las características Administración de dispositivos móviles y Administración de vulnerabilidades y parches.<br>Las causas de este evento y las maneras de responder son las siguientes:<br>• El periodo de vigencia de la licencia ha caducado. Agregue una licencia que permita usar el modo de funcionalidad completa de Kaspersky Security Center (agregue un código de activación válido o un archivo de clave en el Servidor de administración).<br>• El Servidor de administración gestiona más dispositivos de los que permite el límite de la licencia. Mueva los dispositivos de los grupos de administración de un Servidor de administración a los grupos de administración de otro Servidor de administración (si el límite de licencia del otro Servidor de administración lo admite). | 180 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **La licencia está por caducar** | 4129 | KLSRV_EV_LICENSE_SRV_EXPIRE_SOON | Este tipo de evento ocurre cuando se acerca la fecha de caducidad de una licencia comercial.<br>Kaspersky Security Center verifica una vez al día si alguna licencia está próxima a caducar. Los eventos de este tipo se publican 30 días, 15 días, 5 días y 1 día antes de la fecha de caducidad de la licencia. El número de días no se puede modificar. Si el Servidor de administración se encuentra apagado el día especificado antes de la fecha de caducidad de la licencia, el evento no se publicará sino hasta el día siguiente.<br>Cuando caduca la licencia comercial, Kaspersky Security Center solo brinda acceso a las funciones básicas.<br>Puede responder al evento de los siguientes modos:<br>• Asegúrese de tener una clave de licencia de reserva agregada en el Servidor de administración.<br>• Si usa una suscripción, no olvide renovarla. Una suscripción ilimitada se renueva automáticamente si el proveedor de servicios recibe a término y por adelantado el pago correspondiente. | 180 días |
| **El certificado ha caducado** | 4132 | KLSRV_CERTIFICATE_EXPIRED | Los eventos de este tipo ocurren cuando caduca el certificado cliente en los dispositivos móviles. | 180 días |
| **El certificado del servidor de administración ha caducado.** | 6129 | ServerCertificateExpired | Este tipo de evento ocurre cuando caducan los certificados del Servidor de administración para los dispositivos móviles y dispositivos UEFI.<br>Deberá actualizar el certificado caducado. | 180 días |
| **Se revocaron las actualizaciones de los módulos de la aplicación de Kaspersky** | 4142 | KLSRV_SEAMLESS_UPDATE_REVOKED | Este tipo de evento ocurre cuando los especialistas técnicos de Kaspersky revocan una actualización sin interrupciones (tales actualizaciones tienen el estado *Revocada*) y resulta necesario, por ejemplo, actualizar a una versión más nueva. El evento afecta a los parches de Kaspersky Security Center, pero no a los módulos de las aplicaciones de Kaspersky administradas. La razón por la que no se instaló la actualización sin interrupciones se indica en el evento. | 180 días |
| **Auditoría: la exportación a SIEM produjo un error** | 5130 | KLAUD_EV_SIEM_EXPORT_ERROR | Los eventos de este tipo ocurren cuando la exportación de eventos al sistema SIEM falla debido a un error de conexión con el sistema SIEM. | 180 días |

## Eventos del Servidor de administración: nivel Error funcional

En la siguiente tabla, se enumeran los tipos de eventos del Servidor de administración de Kaspersky Security Center que tienen el nivel de importancia **Error funcional**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Para el Servidor de administración, también puede ver y configurar la lista de eventos en las propiedades del Servidor de administración. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Servidor de administración: nivel Error funcional

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Error en tiempo de ejecución** | 4125 | KLSRV_RUNTIME_ERROR | Los eventos de este tipo ocurren debido a problemas desconocidos.<br>En la mayoría de los casos, estos son problemas de DBMS, problemas de red y otros problemas de software y hardware.<br>Los detalles del evento se pueden encontrar en la descripción del evento. | 180 días |
| **Límite de instalaciones excedido en uno de los grupos de aplicaciones con licencia** | 4126 | KLSRV_INVLICPROD_EXCEDED | El Servidor de administración genera eventos de este tipo periódicamente (cada una hora). Los eventos de este tipo ocurren si administra claves de licencia de aplicaciones de terceros en Kaspersky Security Center y si el número de instalaciones ha superado el límite establecido por la clave de licencia de la aplicación de terceros.<br>Puede responder al evento de los siguientes modos:<br>• Revise la lista de dispositivos administrados. Si la aplicación del tercero no se está utilizando en algún dispositivo, desinstálela de ese equipo.<br>• Solicite al tercero una licencia para más dispositivos.<br>Para administrar las claves de licencia de sus aplicaciones de terceros, puede utilizar la característica de grupos de aplicaciones con licencia. Un grupo de aplicaciones con licencia está formado por aplicaciones de terceros que cumplen con los criterios que usted define. | 180 días |
| **Error al sondear el segmento de la nube** | 4143 | KLSRV_KLCLOUD_SCAN_ERROR | Los eventos de este tipo ocurren cuando el Servidor de administración no puede sondear un segmento de red en un entorno de nube. Lea los detalles en la descripción del evento y responda en consecuencia. | No se almacena |
| **Error al copiar las actualizaciones a la carpeta especificada** | 4123 | KLSRV_UPD_REPL_FAIL | Los eventos de este tipo se producen cuando las actualizaciones de software se copian en una carpeta compartida adicional.<br>Puede responder al evento de los siguientes modos:<br>• Verifique si la cuenta de usuario que se emplea para obtener acceso a la(s) carpeta(s) tiene permiso de escritura.<br>• Compruebe si se cambiaron nombre de usuario o contraseña de las carpetas.<br>• Compruebe la conexión a Internet, ya que podría ser la causa del evento. Siga las instrucciones para actualizar las bases de datos y los módulos de software. | 180 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **No queda espacio libre en disco** | 4107 | KLSRV_DISK_FULL | Los eventos de este tipo ocurren cuando el disco duro del dispositivo donde está instalado el Servidor de administración se queda sin espacio libre.<br>Libere espacio en el disco del dispositivo. | 180 días |
| **La carpeta compartida no está disponible** | 4108 | KLSRV_SHARED_FOLDER_UNAVAILABLE | Los eventos de este tipo se producen si la carpeta compartida del Servidor de administración no está disponible.<br>Puede responder al evento de los siguientes modos:<br>• Compruebe si el Servidor de administración (donde se encuentra la carpeta compartida) está encendido y disponible.<br>• Compruebe si se cambió/cambiaron un nombre de usuario y / o una contraseña de la carpeta.<br>• Compruebe la conexión de red. | 180 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **La base de datos del Servidor de administración no está disponible** | 4109 | KLSRV_DATABASE_UNAVAILABLE | Los eventos de este tipo ocurren si la base de datos del Servidor de administración deja de estar disponible.<br>Puede responder al evento de los siguientes modos:<br>• Compruebe si el servidor remoto que tiene instalado SQL Server está disponible.<br>• Vea los registros de DBMS para descubrir el motivo de la falta de disponibilidad de la base de datos del Servidor de administración. Por ejemplo, debido al mantenimiento preventivo, un servidor remoto con SQL Server instalado puede no estar disponible. | 180 días |
| **No hay espacio libre en la base de datos del Servidor de administración** | 4110 | KLSRV_DATABASE_FULL | Los eventos de este tipo ocurren cuando no hay espacio libre en la base de datos del Servidor de administración.<br>El Servidor de administración no funciona cuando su base de datos ha alcanzado su capacidad y cuando no es posible realizar un nuevo registro en la base de datos.<br>Las siguientes son las causas de este evento (agrupadas por DBMS) y distintas maneras en las que puede responder al mismo:<br>• Si su DBMS es SQL Server Express Edition:<br>En la documentación de SQL Server Express, revise el límite de tamaño de la base de datos de la versión que usa. Probablemente su base de datos del Servidor de administración haya excedido el límite de tamaño de la base de datos.<br>Limite el número de eventos que se almacenan en la base de datos del Servidor de administración.<br>La base de datos del Servidor de administración contiene demasiados eventos enviados por el componente Control de aplicaciones. Puede cambiar la configuración de la directiva de Kaspersky Endpoint Security para Windows relacionada con el almacenamiento de eventos de Control de aplicaciones en la base de datos del Servidor de administración.<br>• Si su DBMS no es SQL Server Express Edition:<br>No limite el número de eventos para almacenar en la base de datos del Servidor de administración.<br>Reduzca la lista de eventos para almacenar en la base de datos del Servidor de administración.<br>Revise la información sobre la selección del DBMS. | 180 días |

## Eventos del Servidor de administración: nivel Advertencia

En la siguiente tabla, se enumeran los eventos del Servidor de administración de Kaspersky Security Center que tienen el nivel de importancia **Advertencia**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Para el Servidor de administración, también puede ver y configurar la lista de eventos en las propiedades del Servidor de administración. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Servidor de administración: nivel Advertencia

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Se detectó un evento frecuente** | | KLSRV_EVENT_SPAM_EVENTS_DETECTED | Este tipo de evento ocurre cuando el Servidor de administración detecta un evento frecuente en un dispositivo administrado. Consulte la siguiente sección para obtener más información: Bloquear eventos frecuentes. | 90 días |
| **Se ha superado el límite de la licencia** | 4098 | KLSRV_EV_LICENSE_CHECK_100_110 | Una vez al día, Kaspersky Security Center comprueba si se superó algún límite de licencia.<br>Este tipo de evento ocurre cuando el Servidor de administración detecta que las aplicaciones de Kaspersky instaladas en los dispositivos cliente han superado algún límite de sus licencias y se ha utilizado entre un 100 % y un 110 % del total de unidades con licencia cubiertas por una sola licencia.<br>Los dispositivos cliente se mantienen protegidos aun cuando ocurre este evento.<br>Puede responder al evento de los siguientes modos:<br>• Revise la lista de dispositivos administrados. Elimine los dispositivos que no estén en uso.<br>• Agregue una licencia para más dispositivos (agregue un código de activación válido o un archivo de clave en el Servidor de administración).<br>Kaspersky Security Center determina las reglas para generar eventos cuando se supera un límite de licencia. | 90 días |
| **El dispositivo ha estado inactivo en la red por mucho tiempo** | 4103 | KLSRV_EVENT_HOSTS_NOT_VISIBLE | Este tipo de evento ocurre cuando un dispositivo administrado se encuentra inactivo durante cierto tiempo.<br>La mayoría de las veces, esto sucede porque el dispositivo se ha dado de baja.<br>Puede responder al evento de los siguientes modos:<br>• Elimine el dispositivo manualmente de la lista de dispositivos administrados.<br>• Defina el intervalo de tiempo después del cual se creará el evento **El dispositivo ha estado inactivo en la red por mucho tiempo** mediante la Consola de administración o Kaspersky Security Center Web Console.<br>• Defina el intervalo de tiempo después del cual el dispositivo se eliminará automáticamente del grupo mediante la Consola de administración o Kaspersky Security Center Web Console. | 90 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Conflicto de nombres de dispositivo** | 4102 | KLSRV_EVENT_HOSTS_CONFLICT | Este tipo de evento ocurre cuando el Servidor de administración considera que dos o más dispositivos administrados son un mismo dispositivo.<br>A menudo, esto sucede cuando se utiliza un disco duro clonado para desplegar aplicaciones en los dispositivos administrados, pero el Agente de red del dispositivo de referencia no estaba puesto en el modo de clonación de disco dedicado.<br>Para evitar este problema, ponga el Agente de red en modo de clonación de disco en el dispositivo de referencia antes de clonar el disco duro de ese dispositivo. | 90 días |
| **El estado del dispositivo es Advertencia** | 4114 | KLSRV_HOST_STATUS_WARNING | Este tipo de evento ocurre cuando se le asigna el estado *Advertencia* a un dispositivo administrado. Puede configurar las condiciones en las cuales el estado del dispositivo se cambia a *Advertencia*. | 90 días |
| **El límite de instalaciones está por excederse en uno de los grupos de aplicaciones con licencia** | 4127 | KLSRV_INVLICPROD_FILLED | Este tipo de evento ocurre cuando el número de instalaciones para las aplicaciones de terceros incluidas en un grupo de aplicaciones con licencia alcanza el 90 % del valor máximo permitido en las propiedades de la clave de licencia.<br>Puede responder al evento de los siguientes modos:<br>• Si la aplicación de terceros no se utiliza en algunos de los dispositivos administrados, elimínela de esos dispositivos.<br>• Si estima que la cantidad de instalaciones para la aplicación de terceros superará el máximo permitido en un futuro próximo, considere contactarse con el tercero antes de que eso suceda para obtener una licencia para una cantidad de dispositivos mayor.<br>Para administrar las claves de licencia de sus aplicaciones de terceros, puede utilizar la característica de grupos de aplicaciones con licencia. | 90 días |
| **Se solicitó el certificado** | 4133 | KLSRV_CERTIFICATE_REQUESTED | Este tipo de evento ocurre cuando un certificado de la característica Administración de dispositivos móviles no se vuelve a emitir automáticamente.<br>Estas pueden ser las causas del evento y las respuestas adecuadas:<br>• Se intentó reemitir automáticamente un certificado para el que estaba deshabilitada la opción **Volver a emitir certificados automáticamente si es posible**. Esto puede deberse a un error ocurrido durante la creación del certificado. Es posible que se requiera la reemisión manual del certificado.<br>• Si ha configurado la integración con una infraestructura de claves públicas, la causa podría ser la falta de un atributo SAM-Account-Name de la cuenta utilizada para la integración con dicha infraestructura y para la emisión del certificado. Revise las propiedades de la cuenta. | 90 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Se eliminó el certificado** | 4134 | KLSRV_CERTIFICATE_REMOVED | Este tipo de evento ocurre cuando un administrador elimina un certificado de cualquier tipo (general, de correo o de VPN) para Administración de dispositivos móviles.<br>Después de que se elimina un certificado, los dispositivos móviles que lo habían utilizado para conectarse pierden la capacidad de establecer conexión con el Servidor de administración.<br>Este evento puede resultar útil a la hora de investigar fallas asociadas con la administración de dispositivos móviles. | 90 días |
| **El certificado está por caducar.** | 6128 | ServerCertificateExpiresSoon | Este tipo de evento ocurre cuando caducan los certificados del Servidor de administración para los dispositivos móviles y dispositivos UEFI.<br>Deberá actualizar el certificado caducado. | 90 días |
| **El certificado de APNs caducó** | 4135 | KLSRV_APN_CERTIFICATE_EXPIRED | Este tipo de evento ocurre cuando caduca un certificado de APNs.<br>Debe renovar manualmente el certificado de APNs e instalarlo en un servidor de MDM para iOS. | No se almacena |
| **El certificado de APNs caducará pronto** | 4136 | KLSRV_APN_CERTIFICATE_EXPIRES_SOON | Este tipo de evento ocurre cuando quedan menos de catorce días para que caduque el certificado de APNs.<br>Cuando el certificado de APNs caduque, deberá renovarlo manualmente e instalarlo en un servidor de MDM para iOS.<br>Le recomendamos que programe la renovación del certificado de APNs para antes de la fecha de caducidad. | No se almacena |
| **No se pudo enviar el mensaje de FCM al dispositivo móvil** | 4138 | KLSRV_GCM_DEVICE_ERROR | Los eventos de este tipo ocurren cuando la Administración de dispositivos móviles está configurada para usar Firebase Cloud Messaging (FCM) para conectarse a dispositivos móviles administrados con un sistema operativo Android y el servidor de FCM no puede manejar algunas de las solicitudes recibidas del Servidor de administración. Lo que esto significa es que algunos de los dispositivos móviles administrados no recibirán una notificación push.<br>Lea el código HTTP en los detalles de la descripción del evento y responda en consecuencia. Para obtener más información sobre los códigos HTTP recibidos del servidor de FCM y los errores relacionados, consulte la documentación del servicio Firebase (en especial, el capítulo "Códigos de respuesta de errores de mensajes descendentes"). | 90 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Error de HTTP al enviar un mensaje del FCM al servidor de FCM** | 4139 | KLSRV_GCM_HTTP_ERROR | Los eventos de este tipo ocurren cuando la Administración de dispositivos móviles está configurada para usar Firebase Cloud Messaging (FCM) para conectar dispositivos móviles administrados con el sistema operativo Android y el servidor de FCM devuelve al Servidor de administración una solicitud con un código HTTP distinto de 200 (OK).<br>Estas pueden ser las causas del evento y las respuestas adecuadas:<br>• Problemas en el servidor de FCM. Lea el código HTTP en los detalles de la descripción del evento y responda en consecuencia. Para obtener más información sobre los códigos HTTP recibidos del servidor de FCM y los errores relacionados, consulte la documentación del servicio Firebase (en especial, el capítulo "Códigos de respuesta de errores de mensajes descendentes").<br>• Problemas en el servidor proxy (si usa un servidor proxy). Lea el código HTTP en los detalles de la descripción del evento y responda en consecuencia. | 90 días |
| **No se pudo enviar el mensaje de FCM al servidor de FCM** | 4140 | KLSRV_GCM_GENERAL_ERROR | Este tipo de evento ocurre cuando suceden errores inesperados del lado del Servidor de administración al utilizar el protocolo HTTP de Firebase Cloud Messaging.<br>Lea los detalles en la descripción del evento y responda en consecuencia.<br>Si no puede encontrar la solución a un problema por su cuenta, le recomendamos que se comunique con el servicio de soporte técnico de Kaspersky. | 90 días |
| **Queda poco espacio libre en el disco duro** | 4105 | KLSRV_NO_SPACE_ON_VOLUMES | Este tipo de evento ocurre cuando se agota el espacio en el disco duro del dispositivo en el que está instalado el Servidor de administración.<br>Libere espacio en el disco del dispositivo. | 90 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Queda poco espacio libre en la base de datos del Servidor de administración** | 4106 | KLSRV_NO_SPACE_IN_DATABASE | Este tipo de evento ocurre cuando el espacio disponible en la base de datos del Servidor de administración es demasiado limitado. De no resolverse esta situación, la base de datos del Servidor de administración alcanzará rápidamente su límite de capacidad y el Servidor de la administración dejará de funcionar.<br>Las siguientes son las causas de este evento (agrupadas por DBMS) y las distintas maneras en las que puede responder.<br>Si su DBMS es SQL Server Express Edition:<br>• En la documentación de SQL Server Express, revise el límite de tamaño de la base de datos de la versión que usa. Es probable que la base de datos del Servidor de administración esté a punto de alcanzar el tamaño máximo posible.<br>• Limite el número de eventos que se almacenan en la base de datos del Servidor de administración.<br>• La base de datos del Servidor de administración contiene demasiados eventos enviados por el componente Control de aplicaciones. Puede cambiar la configuración de la directiva de Kaspersky Endpoint Security para Windows relacionada con el almacenamiento de eventos de Control de aplicaciones en la base de datos del Servidor de administración.<br>Si su DBMS no es SQL Server Express Edition:<br>• No limite el número de eventos que se almacenan en la base de datos del Servidor de administración.<br>• Reduzca la lista de eventos que se almacenan en la base de datos del Servidor de administración.<br>Revise la información sobre la selección del DBMS. | 90 días |
| **Se ha interrumpido la conexión con el Servidor de administración secundario** | 4116 | KLSRV_EV_SLAVE_SRV_DISCONNECTED | Este tipo de evento ocurre cuando se interrumpe una conexión con el Servidor de administración secundario.<br>Consulte el registro de eventos de Kaspersky en el dispositivo en el que esté instalado el Servidor de administración secundario y responda en consecuencia. | 90 días |
| **Se ha interrumpido la conexión con el Servidor de administración principal** | 4118 | KLSRV_EV_MASTER_SRV_DISCONNECTED | Este tipo de evento ocurre cuando se interrumpe una conexión con el Servidor de administración principal.<br>Consulte el registro de eventos de Kaspersky en el dispositivo en el que esté instalado el Servidor de administración principal y responda en consecuencia. | 90 días |
| **Se registraron nuevas actualizaciones para los módulos de la aplicación de Kaspersky** | 4141 | KLSRV_SEAMLESS_UPDATE_REGISTERED | Este tipo de evento ocurre cuando el Servidor de administración registra nuevas actualizaciones para el software de Kaspersky instalado en los dispositivos administrados y se necesita que usted apruebe la instalación de esas actualizaciones.<br>Apruebe o rechace las actualizaciones mediante la Consola de administración o a través de Kaspersky Security Center Web Console. | 90 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Se superó el límite del número de eventos en la base de datos, se inició la eliminación de eventos** | 4145 | KLSRV_EVP_DB_TRUNCATING | Este tipo de evento ocurre cuando el sistema comienza a eliminar eventos antiguos de la base de datos del Servidor de administración por haberse alcanzado el límite de capacidad de la misma.<br>Puede responder al evento de los siguientes modos:<br>• Cambie el número de eventos que se conservará, como máximo, en la base de datos del Servidor de administración.<br>• Reduzca la lista de eventos que se almacenan en la base de datos del Servidor de administración. | No se almacena |
| **Se superó el límite del número de eventos en la base de datos, se eliminó los eventos** | 4146 | KLSRV_EVP_DB_TRUNCATED | Este tipo de evento ocurre cuando el sistema eliminó eventos antiguos de la base de datos del Servidor de administración por haberse alcanzado el límite de capacidad de la misma.<br>Puede responder al evento de los siguientes modos:<br>• Cambie el número de eventos que se conservará, como máximo, en la base de datos del Servidor de administración.<br>• Reduzca la lista de eventos que se almacenan en la base de datos del Servidor de administración. | No se almacena |
| **Auditoría (la prueba de conexión al servidor de SIEM produjo un error)** | 5120 | KLAUD_EV_SIEM_TEST_FAILED | Los eventos de este tipo se producen cuando falla una conexión de prueba al servidor SIEM. | 30 días |
| **No se pudo emitir el certificado automáticamente** | | KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR | Este evento ocurre en caso de un error al crear un certificado de cliente para un dispositivo móvil (un dispositivo que opera bajo un protocolo móvil). | 90 días |

## Eventos del Servidor de administración: nivel Información

En la siguiente tabla, se enumeran los eventos del Servidor de administración de Kaspersky Security Center que tienen el nivel de importancia **Información**.

Eventos del Servidor de administración: nivel Información

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado | Observaciones |
|---|---|---|---|---|
| **Se ha consumido más del 90 % de la clave de licencia** | 4097 | KLSRV_EV_LICENSE_CHECK_90 | 30 días | |
| **Se detectó un nuevo dispositivo** | 4100 | KLSRV_EVENT_HOSTS_NEW_DETECTED | 30 días | |
| **Dispositivo agregado al grupo automáticamente** | 4101 | KLSRV_EVENT_HOSTS_NEW_REDIRECTED | 30 días | |
| **El dispositivo se movió automáticamente de acuerdo con una regla** | 1074 | KLSRV_HOST_MOVED_WITH_RULE_EX | 30 días | |
| **Dispositivo eliminado del grupo: estuvo inactivo en la red por mucho tiempo** | 4104 | KLSRV_INVISIBLE_HOSTS_REMOVED | 30 días | |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado | Observaciones |
|---|---|---|---|---|
| **El límite de instalaciones está por alcanzarse (se consumió más del 95 %) en uno de los grupos de aplicaciones con licencia** | 4128 | KLSRV_INVLICPROD_EXPIRED_SOON | 30 días | |
| **Se han encontrado archivos para enviar a Kaspersky para su análisis** | 4131 | KLSRV_APS_FILE_APPEARED | 30 días | |
| **El id. de instancia de FCM ha cambiado en este dispositivo móvil** | 4137 | KLSRV_GCM_DEVICE_REGID_CHANGED | 30 días | |
| **Las actualizaciones se copiaron correctamente en la carpeta especificada** | 4122 | KLSRV_UPD_REPL_OK | 30 días | |
| **Se estableció la conexión con el Servidor de administración secundario** | 4115 | KLSRV_EV_SLAVE_SRV_CONNECTED | 30 días | |
| **Se estableció la conexión con el Servidor de administración principal** | 4117 | KLSRV_EV_MASTER_SRV_CONNECTED | 30 días | |
| **Las bases de datos se han actualizado** | 4144 | KLSRV_UPD_BASES_UPDATED | 30 días | |
| **Auditoría: Se estableció la conexión con el Servidor de administración** | 4147 | KLAUD_EV_SERVERCONNECT | 30 días | |
| **Auditoría: El objeto se modificó** | 4148 | KLAUD_EV_OBJECTMODIFY | 30 días | Este evento responde a cambios ocurridos en los siguientes objetos:<br>• Grupo de administración<br>• Grupo de seguridad<br>• Usuario<br>• Paquete<br>• Tarea<br>• Directiva<br>• Servidores<br>• Servidor virtual |
| **Auditoría: El estado del objeto se modificó** | 4150 | KLAUD_EV_TASK_STATE_CHANGED | 30 días | Este evento ocurre, por ejemplo, cuando una tarea no se completa debido a un error. |
| **Auditoría: La configuración del grupo se modificó** | 4149 | KLAUD_EV_ADMGROUP_CHANGED | 30 días | |
| **Auditoría: Se cerró la conexión con el Servidor de administración** | 4151 | KLAUD_EV_SERVERDISCONNECT | 30 días | |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado | Observaciones |
|---|---|---|---|---|
| **Auditoría: Las propiedades del objeto se han modificado** | 4152 | KLAUD_EV_OBJECTPROPMODIFIED | 30 días | Este evento responde a cambios ocurridos en las siguientes propiedades:<br>• Usuario<br>• Licencia<br>• Servidores<br>• Servidor virtual |
| **Auditoría: Las propiedades del usuario se han modificado** | 4153 | KLAUD_EV_OBJECTACLMODIFIED | 30 días | |
| **Auditoría: Se importaron o exportaron claves de cifrado del Servidor de administración** | 5100 | KLAUD_EV_DPEKEYSEXPORT | 30 días | |
| **Auditoría (la prueba de conexión al servidor de SIEM se realizó correctamente)** | 5110 | KLAUD_EV_SIEM_TEST_SUCCESS | 30 días | Los eventos de este tipo se producen cuando se logra establecer una conexión de prueba con el servidor SIEM. |
| **Certificado de reserva creado** | | ServerReserveCertificateCreated | 30 días | Este evento se produce cuando se crea un certificado del Servidor de administración. |
| **Renovación del certificado** | | ServerCertificateRenewed | 30 días | Este evento ocurre cuando se renueva el certificado del Servidor de administración. |
| **El certificado se emitió correctamente de forma automática** | | KLSRV_CERTIFICATE_AUTO_ISSUED | 30 días | Este evento ocurre cuando se creó exitosamente un certificado para un dispositivo móvil (un dispositivo que opera bajo un protocolo móvil). |

Los eventos **Certificado de reserva creado, Renovación del certificado** y **El certificado se emitió correctamente de forma automática** son publicados automáticamente por el Servidor de administración, y aparecen en la Consola de administración únicamente cuando las operaciones correspondientes a dichos eventos se realizan sobre los certificados del Servidor de administración para dispositivos con certificado móvil y dispositivos UEFI.

# Eventos del Agente de red

En esta sección, se brinda información sobre los eventos relacionados con el Agente de red.

## Eventos del Agente de red: nivel Error funcional

En la siguiente tabla, se enumeran los tipos de eventos del Agente de red de Kaspersky Security Center que tienen el nivel de gravedad **Error funcional**.

Puede definir los ajustes de notificación y los ajustes de almacenamiento para cada uno de los eventos que pueda generar una aplicación; para ello debe dirigirse a la pestaña **Configuración de eventos** en la directiva de la aplicación. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Error de instalación de la actualización** | 7702 | KLNAG_EV_PATCH_INSTALL_ERROR | Los eventos de este tipo se producen si la actualización automática y la aplicación de parches para los componentes de Kaspersky Security Center no tuvieron éxito. El evento no está vinculado a la actualización de las aplicaciones de Kaspersky administradas.<br>Lea la descripción del evento. El evento puede tener su origen en un problema de Windows ocurrido en el Servidor de administración. Si la descripción menciona algún problema con la configuración de Windows, resuelva ese problema. | 30 días |
| **Error al instalar la actualización de software de terceros** | 7697 | KLNAG_EV_3P_PATCH_INSTALL_ERROR | Los eventos de este tipo se producen si las funciones de Administración de vulnerabilidades y parches y Administración de dispositivos móviles están en uso y si la actualización del software de terceros no se realizó correctamente.<br>Compruebe si el enlace al software desarrollado por el tercero es válido. Lea la descripción del evento. | 30 días |
| **Error al instalar las actualizaciones de Windows Update** | 7717 | KLNAG_EV_WUA_INSTALL_ERROR | Este tipo de evento ocurre cuando no se pueden instalar las actualizaciones de Windows. Configurar las actualizaciones de Windows en una directiva del Agente de red.<br>Lea la descripción del evento. Busque el error en Microsoft Knowledge Base. Póngase en contacto con el servicio de soporte técnico de Microsoft si no puede resolver el problema por su cuenta. | 30 días |
| **Administración de usuarios: errores** | 7723 | KLNAG_EV_USR_MNG_ERR | Evento de advertencia general. | 30 días |
| **No se pudo restaurar el archivo sudoers al valor de referencia** | 7726 | KLNAG_EV_SUDOER_RESTORED_ERR | El evento contiene la descripción correspondiente al error de reemplazo del archivo sudoers. | 30 días |
| **No se pudieron instalar los certificados raíz** | 7728 | KLNAG_EV_ROOT_CERT_INSTALL_ERR | El evento contiene la descripción correspondiente al error de instalación de los certificados. | 30 días |
| **No se pudieron eliminar los certificados raíz** | 7730 | KLNAG_EV_ROOT_CERT_REMOVE_ERR | El evento contiene la descripción correspondiente al error de eliminación de certificados. | 30 días |

## Eventos del Agente de red: nivel Advertencia

La siguiente tabla muestra los eventos del Agente de red de Kaspersky Security Center Linux que tienen el nivel de gravedad **Advertencia**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Agente de red: nivel Advertencia

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado |
|---|---|---|---|
| **Se ha devuelto una advertencia durante la instalación de la actualización del módulo de software** | 7701 | KLNAG_EV_PATCH_INSTALL_WARNING | 30 días |
| **La instalación de la actualización de software de terceros se ha completado con una advertencia** | 7696 | KLNAG_EV_3P_PATCH_INSTALL_WARNING | 30 días |
| **La instalación de la actualización de software de terceros se ha pospuesto** | 7698 | KLNAG_EV_3P_PATCH_INSTALL_SLIPPED | 30 días |
| **Ocurrió un problema de seguridad** | 549 | GNRL_EV_APP_INCIDENT_OCCURED | 30 días |
| **Se inició el Proxy de KSN. No se pudo comprobar la disponibilidad de KSN** | 7718 | KSNPROXY_STARTED_CON_CHK_FAILED | 30 días |
| **Administración de usuarios: advertencias** | 7722 | KLNAG_EV_USR_MNG_WRN | 30 días |
| **El archivo sudoers encontrado no coincide con el valor de referencia** | 7724 | KLNAG_EV_SUDOER_DIFFERENT | 30 días |

## Eventos del Agente de red: nivel Información

La siguiente tabla muestra los eventos del Agente de red de Kaspersky Security Center Linux que tienen el nivel de gravedad **Información**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Agente de red: nivel Información

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado |
|---|---|---|---|
| **La actualización para los módulos de software se instaló correctamente** | 7699 | KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY | 30 días |
| **Se ha iniciado la instalación de la actualización para los módulos de software** | 7700 | KLNAG_EV_PATCH_INSTALL_STARTING | 30 días |
| **Se instaló una aplicación** | 7703 | KLNAG_EV_INV_APP_INSTALLED | 30 días |
| **Se desinstaló una aplicación** | 7704 | KLNAG_EV_INV_APP_UNINSTALLED | 30 días |
| **Se instaló una aplicación supervisada** | 7705 | KLNAG_EV_INV_OBS_APP_INSTALLED | 30 días |
| **Se desinstaló una aplicación supervisada** | 7706 | KLNAG_EV_INV_OBS_APP_UNINSTALLED | 30 días |
| **Se instaló una aplicación de terceros** | 7707 | KLNAG_EV_INV_CMPTR_APP_INSTALLED | 30 días |
| **Nuevo dispositivo agregado** | 7708 | KLNAG_EV_DEVICE_ARRIVAL | 30 días |
| **Dispositivo eliminado** | 7709 | KLNAG_EV_DEVICE_REMOVE | 30 días |
| **Se detectó un nuevo dispositivo** | 7710 | KLNAG_EV_NAC_DEVICE_DISCOVERED | 30 días |
| **Dispositivo autorizado** | 7711 | KLNAG_EV_NAC_HOST_AUTHORIZED | 30 días |
| **Windows Desktop Sharing: el archivo ha sido leído** | 7712 | KLUSRLOG_EV_FILE_READ | 30 días |
| **Windows Desktop Sharing: el archivo ha sido modificado** | 7713 | KLUSRLOG_EV_FILE_MODIFIED | 30 días |
| **Windows Desktop Sharing: la aplicación ha sido iniciada** | 7714 | KLUSRLOG_EV_PROCESS_LAUNCHED | 30 días |
| **Windows Desktop Sharing: iniciado** | 7715 | KLUSRLOG_EV_WDS_BEGIN | 30 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado |
|---|---|---|---|
| **Windows Desktop Sharing: detenido** | 7716 | KLUSRLOG_EV_WDS_END | 30 días |
| **La actualización de software de terceros se ha instalado correctamente** | 7694 | KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY | 30 días |
| **Se ha iniciado la instalación de la actualización de software de terceros** | 7695 | KLNAG_EV_3P_PATCH_INSTALL_STARTING | 30 días |
| **El proxy de KSN se ha iniciado. La disponibilidad de KSN se verificó correctamente** | 7719 | KSNPROXY_STARTED_CON_CHK_OK | 30 días |
| **El Proxy de KSN se detuvo** | 7720 | KSNPROXY_STOPPED | 30 días |

# Eventos del Servidor de MDM para iOS

Esta sección contiene información sobre los eventos relacionados con el Servidor de MDM para iOS.

## Eventos de errores funcionales del Servidor de MDM para iOS

La siguiente tabla muestra los eventos del servidor de MDM para iOS de Kaspersky Security Center que tienen el nivel de gravedad **Error funcional**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos de errores funcionales del Servidor de MDM para iOS

| Nombre que se muestra para el tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado |
|---|---|---|
| **Error al solicitar la lista de perfiles** | PROFILELIST_COMMAND_FAILED | 30 días |
| **Error al instalar perfil** | INSTALLPROFILE_COMMAND_FAILED | 30 días |
| **Error al eliminar el perfil** | REMOVEPROFILE_COMMAND_FAILED | 30 días |
| **Error al solicitar la lista de perfiles de aprovisionamiento** | PROVISIONINGPROFILELIST_COMMAND_FAILED | 30 días |
| **Error al instalar perfil de aprovisionamient** | INSTALLPROVISIONINGPROFILE_COMMAND_FAILED | 30 días |
| **Error al eliminar perfil de aprovisionamiento** | REMOVEPROVISIONINGPROFILE_COMMAND_FAILED | 30 días |
| **Error al solicitar la lista de certificados digitales** | CERTIFICATELIST_COMMAND_FAILED | 30 días |
| **Error al solicitar la lista de aplicaciones instaladas** | INSTALLEDAPPLICATIONLIST_COMMAND_FAILED | 30 días |
| **Error al solicitar información general sobre el dispositivo móvil** | DEVICEINFORMATION_COMMAND_FAILED | 30 días |
| **Error al solicitar la información de seguridad** | SECURITYINFO_COMMAND_FAILED | 30 días |
| **No se pudo bloquear el dispositivo móvil** | DEVICELOCK_COMMAND_FAILED | 30 días |
| **Error al restablecer la contraseña** | CLEARPASSCODE_COMMAND_FAILED | 30 días |
| **Error al eliminar los datos del dispositivo móvil** | ERASEDEVICE_COMMAND_FAILED | 30 días |
| **No se pudo instalar la app** | INSTALLAPPLICATION_COMMAND_FAILED | 30 días |
| **Error al establecer el código de canje para la app** | APPLYREDEMPTIONCODE_COMMAND_FAILED | 30 días |

| Nombre que se muestra para el tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado |
|---|---|---|
| **Error al solicitar la lista de apps administradas** | MANAGEDAPPLICATIONLIST_COMMAND_FAILED | 30 días |
| **No se pudo eliminar la app administrada** | REMOVEAPPLICATION_COMMAND_FAILED | 30 días |
| **La configuración de roaming se ha rechazado** | SETROAMINGSETTINGS_COMMAND_FAILED | 30 días |
| **Se produjo un error en la operación de la app** | PRODUCT_FAILURE | 30 días |
| **El resultado del comando contiene datos no válidos** | MALFORMED_COMMAND | 30 días |
| **Error al enviar la notificación push** | SEND_PUSH_NOTIFICATION_FAILED | 30 días |
| **No se puede enviar el comando** | SEND_COMMAND_FAILED | 30 días |
| **Dispositivo no encontrado** | DEVICE_NOT_FOUND | 30 días |

## Eventos de advertencia del servidor de MDM para iOS

La siguiente tabla muestra los eventos del servidor de MDM para iOS de Kaspersky Security Center que tienen el nivel de gravedad **Advertencia**.

Puede definir los ajustes de notificación y los ajustes de almacenamiento para cada uno de los eventos que pueda generar una aplicación; para ello debe dirigirse a la pestaña **Configuración de eventos** en la directiva de la aplicación. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos de advertencia del servidor de MDM para iOS

| Nombre que se muestra para el tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado |
|---|---|---|
| **Se detectó un intento de conectar un dispositivo móvil bloqueado** | INACTICE_DEVICE_TRY_CONNECTED | 30 días |
| **El perfil se ha eliminado** | MDM_PROFILE_WAS_REMOVED | 30 días |
| **Se detectó un intento de reutilizar un certificado cliente** | CLIENT_CERT_ALREADY_IN_USE | 30 días |
| **Se detectó un dispositivo inactivo** | FOUND_INACTIVE_DEVICE | 30 días |
| **Se requiere el código de canje** | NEED_REDEMPTION_CODE | 30 días |
| **El perfil incluido en la directiva se ha eliminado del dispositivo** | UMDM_PROFILE_WAS_REMOVED | 30 días |

## Eventos informativos del servidor de MDM para iOS

La siguiente tabla muestra los eventos del servidor de MDM para iOS de Kaspersky Security Center que tienen el nivel de gravedad **Información**.

Puede definir los ajustes de notificación y los ajustes de almacenamiento para cada uno de los eventos que pueda generar una aplicación; para ello debe dirigirse a la pestaña **Configuración de eventos** en la directiva de la aplicación. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos informativos del servidor de MDM para iOS

| Nombre que se muestra para el tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado |
|---|---|---|
| **Se conectó un nuevo dispositivo móvil** | NEW_DEVICE_CONNECTED | 30 días |
| **La lista de perfiles se solicitó correctamente** | PROFILELIST_COMMAND_SUCCESSFULL | 30 días |

| Nombre que se muestra para el tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado |
|---|---|---|
| **El perfil se ha instalado correctamente** | INSTALLPROFILE_COMMAND_SUCCESSFULL | 30 días |
| **El perfil se ha eliminado correctamente** | REMOVEPROFILE_COMMAND_SUCCESSFULL | 30 días |
| **La lista de perfiles de aprovisionamiento se solicitó correctamente** | PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL | 30 días |
| **El perfil de aprovisionamiento se ha instalado correctamente** | INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL | 30 días |
| **El perfil de aprovisionamiento se ha eliminado correctamente** | REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL | 30 días |
| **La lista de certificados digitales se solicitó correctamente** | CERTIFICATELIST_COMMAND_SUCCESSFULL | 30 días |
| **La lista de aplicaciones instaladas se solicitó correctamente** | INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL | 30 días |
| **La información general sobre el dispositivo móvil se solicitó correctamente** | DEVICEINFORMATION_COMMAND_SUCCESSFULL | 30 días |
| **La información de seguridad se solicitó correctamente** | SECURITYINFO_COMMAND_SUCCESSFULL | 30 días |
| **El dispositivo móvil se bloqueó correctamente** | DEVICELOCK_COMMAND_SUCCESSFULL | 30 días |
| **La contraseña se restableció correctamente** | CLEARPASSCODE_COMMAND_SUCCESSFULL | 30 días |
| **Los datos del dispositivo móvil se eliminaron correctamente** | ERASEDEVICE_COMMAND_SUCCESSFULL | 30 días |
| **La app se ha instalado correctamente** | INSTALLAPPLICATION_COMMAND_SUCCESSFULL | 30 días |
| **El código de canje se estableció correctamente para la aplicación** | APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL | 30 días |
| **La lista de apps administradas se solicitó correctamente** | MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL | 30 días |
| **La aplicación administrada se eliminó correctamente** | REMOVEAPPLICATION_COMMAND_SUCCESSFULL | 30 días |
| **La configuración de roaming se aplicó correctamente** | SETROAMINGSETTINGS_COMMAND_SUCCESSFUL | 30 días |

# Bloquear eventos frecuentes

Esta sección proporciona información sobre la administración del bloqueo de eventos frecuentes, la eliminación del bloqueo de eventos frecuentes y la exportación de la lista de eventos frecuentes a un archivo.

## Acerca del bloqueo de eventos frecuentes

Una aplicación administrada, por ejemplo, Kaspersky Endpoint Security para Windows, instalada en uno o varios dispositivos administrados puede enviar muchos eventos del mismo tipo al Servidor de administración. La recepción de eventos frecuentes puede sobrecargar la base de datos del Servidor de administración y sobrescribir otros eventos. El Servidor de administración comienza a bloquear los eventos más frecuentes cuando el número de todos los eventos recibidos supera el límite especificado para la base de datos.

El Servidor de administración bloquea la recepción de los eventos frecuentes automáticamente. No puede bloquear los eventos frecuentes usted mismo, ni elegir qué eventos bloquear.

Si quiere saber si un evento está bloqueado, puede verificar si este evento está presente en la sección **Bloqueo de eventos frecuentes** de las propiedades del Servidor de administración. Si el evento está bloqueado, puede hacer lo siguiente:

- Si quiere evitar que se sobrescriba la base de datos, puede seguir bloqueando la recepción de dicho tipo de eventos.
- Por ejemplo, si quiere encontrar el motivo del envío de los eventos frecuentes al Servidor de administración puede desbloquear los eventos frecuentes y seguir recibiendo los eventos de este tipo de todas formas.
- Si quiere seguir recibiendo los eventos frecuentes hasta que se vuelvan a bloquear, puede eliminar el bloqueo de los eventos frecuentes.

## Administrar el bloqueo de eventos frecuentes

El Servidor de administración bloquea automáticamente la recepción de los eventos frecuentes, pero se puede detener el bloqueo y seguir recibiendo los eventos frecuentes. También puede bloquear la recepción de los eventos frecuentes que haya desbloqueado antes.

*Para administrar el bloqueo de eventos frecuentes:*

1. En el árbol de la consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y luego seleccione **Propiedades**.
2. En la ventana de propiedades del Servidor de administración, vaya al panel **Secciones** y, a continuación, seleccione **Bloqueo de eventos frecuentes**.
3. En la sección **Bloqueo de eventos frecuentes**:
   - Seleccione las opciones **Tipo de evento** de los eventos que desea bloquear para que no se reciban.
   - Anule la selección de las opciones **Tipo de evento** de los eventos que desea seguir recibiendo.
4. Haga clic en el botón **Aplicar**.
5. Haga clic en el botón **Aceptar**.

El Servidor de administración recibe los eventos frecuentes para los que anuló la selección de la opción **Tipo de evento** y bloquea la recepción de eventos frecuentes para los que seleccionó la opción **Tipo de evento**.

## Eliminar el bloqueo de eventos frecuentes

Puede eliminar el bloqueo de los eventos frecuentes y empezar a recibirlos hasta que el Servidor de administración vuelva a bloquear este tipo de eventos frecuentes.

*Para eliminar el bloqueo de eventos frecuentes:*

1. En el árbol de la consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y luego seleccione **Propiedades**.
2. En la ventana de propiedades del Servidor de administración, vaya al panel **Secciones** y, a continuación, seleccione **Bloqueo de eventos frecuentes**.

3. En la sección **Bloqueo de eventos frecuentes**, haga clic en la fila del evento frecuente para el que desea eliminar el bloqueo.

4. Haga clic en el botón **Eliminar**.

El evento frecuente se elimina de la lista de eventos frecuentes. El Servidor de administración recibirá los eventos de este tipo.

## Exportar una lista de eventos frecuentes en un archivo

*Para exportar una lista de eventos frecuentes a un archivo:*

1. En el árbol de la consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y luego seleccione **Propiedades**.

2. En la ventana de propiedades del Servidor de administración, vaya al panel **Secciones** y, a continuación, seleccione **Bloqueo de eventos frecuentes**.

3. Haga clic en el botón **Exportar a archivo**.

4. En la ventana **Guardar como** que se abre, especifique la ruta al archivo en el cual desea guardar la lista.

5. Haga clic en el botón **Guardar**.

Todos los registros de la lista de eventos frecuentes se exportan a un archivo.

# Controlar los cambios en el estado de las máquinas virtuales

El Servidor de administración almacena información sobre el estado de los dispositivos administrados, como el registro de hardware y la lista de aplicaciones instaladas, o la configuración de las aplicaciones, tareas y directivas administradas. Si una máquina virtual funciona como un dispositivo administrado, el usuario puede restaurar su estado en cualquier momento con una imagen instantánea anteriormente creada de la máquina virtual. La información sobre el estado de la máquina virtual en el Servidor de administración puede dejar de estar actualizada.

Por ejemplo, el administrador había creado una directiva de protección en el Servidor de administración a las 12:00 p.m., que comenzó a ejecutarse en la máquina virtual VM_1 a las 12:01 p.m. A las 12:30 p.m., el usuario de la máquina virtual VM_1 cambió su estado al restaurarla a partir de una instantánea realizada a las 11:00 a.m. La directiva de protección deja de ejecutarse en la máquina virtual. Sin embargo, la información desactualizada en el Servidor de administración asegura que la directiva de protección en la máquina virtual VM_1 continúa en funcionamiento.

Kaspersky Security Center ayuda a controlar los cambios en el estado de las máquinas virtuales.

Después de cada sincronización con el dispositivo, el Servidor de administración genera un ID único, que se almacena tanto en el dispositivo y en el Servidor de administración. Antes de iniciar la siguiente sincronización, el Servidor de administración compara los valores de esos ID de ambos lados. Si los valores de las ID no coinciden, el Servidor de administración reconoce a la máquina virtual como restaurada de una imagen instantánea. El Servidor de administración restablece toda la configuración de las directivas y tareas activas en la máquina virtual y le envía las directivas actualizadas y la lista de las tareas de grupo.

# Supervisar el estado de la protección antivirus utilizando información del registro del sistema

*Para supervisar el estado de protección antivirus en un dispositivo cliente mediante la información registrada por el Agente de red, según el sistema operativo del dispositivo, realice lo siguiente:*

- En dispositivos con Windows:

  1. Abra el registro del sistema de un dispositivo cliente (por ejemplo, de forma local con el comando regedit desde el menú **Iniciar** → **Ejecutar**).

  2. Vaya al siguiente archivo:

     - Para sistemas de 32 bits:

       HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState

     - Para sistemas de 64 bits:

       HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\Stati

     El registro del sistema muestra información sobre el estado de la protección antivirus del dispositivo cliente.

- En dispositivos con Linux:

  - La información se adjunta en archivos de texto separados, uno para cada tipo de datos, que se encuentran en /var/opt/kaspersky/klnagent/1103/1.0.0.0/Statistics/AVState/.

- En dispositivos con macOS:

  - La información se adjunta en archivos de texto separados, uno para cada tipo de datos, que se encuentran en /Library/Application Support/Kaspersky Lab/klnagent/Data/1103/1.0.0.0/Statistics/AVState/.

El estado de la protección antivirus se corresponde con los valores de las claves descritas en la tabla a continuación.

Claves de registro y sus valores posibles

| Clave (tipo de datos) | Valor | Descripción |
|---|---|---|
| `Protection_LastConnected (REG_SZ)` | MM/DD/AAAA HH-MM-SS | Fecha y hora (en formato UTC) de la última conexión con el Servidor de administración |
| `Protection_AdmServer (REG_SZ)` | IP, nombre DNS o nombre NetBIOS | Nombre del Servidor de administración virtual que administra el dispositivo |
| `Protection_NagentVersion (REG_SZ)` | a.b.c.d | Número de compilación del Agente de red instalado en el dispositivo |
| `Protection_NagentFullVersion (REG_SZ)` | a.b.c.d (parche1; parche2; ...; parcheN) | Número completo de la versión del Agente de red (con parches) instalada en el dispositivo |
| `Protection_HostId (REG_SZ)` | Id. del dispositivo | El id. del dispositivo |
| `Protection_DynamicVM (REG_DWORD)` | 0 — no<br>1 — sí | El Agente de red se instala en el modo dinámico para VDI |
| `Protection_AvInstalled (REG_DWORD)` | 0 — no<br>1 — sí | Una aplicación de seguridad se instala en el dispositivo móvil |

| Clave (tipo de datos) | Valor | Descripción |
|---|---|---|
| `Protection_AvRunning (REG_DWORD)` | 0 — no<br>1 — sí | La protección en tiempo real está activa en el dispositivo |
| `Protection_HasRtp (REG_DWORD)` | 0 — no<br>1 — sí | Un componente de protección en tiempo real está instalado |
| `Protection_RtpState (REG_DWORD)` | Estado de protección en tiempo real: | |
| | 0 | Desconocido |
| | 1 | Desactivada |
| | 2 | En pausa |
| | 3 | Iniciando |
| | 4 | Activado |
| | 5 | Activado con el nivel de protección alto (protección máxima) |
| | 6 | Activado con el nivel de protección bajo (velocidad máxima) |
| | 7 | Activado con la configuración predeterminada (recomendada) |
| | 8 | Activado con la configuración personalizada |
| | 9 | Error de funcionamiento |
| `Protection_LastFscan (REG_SZ)` | MM/DD/AAAA HH-MM-SS | Fecha y hora (en formato UTC) del último análisis completo |
| `Protection_BasesDate (REG_SZ)` | MM/DD/AAAA HH-MM-SS | Fecha y hora (en formato UTC) de la publicación de las bases de datos de la aplicación |

# Ver y configurar las acciones para dispositivos inactivos

Puede recibir una notificación si se detecta que los dispositivos cliente de un grupo están inactivos. También puede hacer que esos dispositivos se eliminen automáticamente.

*Para ver o configurar las acciones que se llevan a cabo cuando los dispositivos de un grupo están inactivos:*

1. En el árbol de la consola, haga clic con el botón derecho en el nombre del grupo de administración requerido.
2. En el menú contextual, seleccione **Propiedades**.

   Esto abre la ventana de propiedades del grupo de administración.
3. En la ventana **Propiedades**, vaya a la sección **Dispositivos**.

4. De ser necesario, habilite o deshabilite las opciones siguientes:

- **Notificar al administrador si el dispositivo ha estado inactivo por más de (días)**

  Cuando esta opción está habilitada y se detecta que un dispositivo ha estado inactivo, el administrador recibe una notificación. Puede especificar el intervalo de tiempo que se deja pasar antes de que se cree el evento **El dispositivo ha estado inactivo en la red por mucho tiempo**. El intervalo de tiempo por defecto es de 7 días.

  Esta opción está activada de forma predeterminada.

- **Eliminar el dispositivo del grupo si ha estado inactivo por más de (días)**

  Si esta opción está habilitada, puede especificar el intervalo de tiempo que se deja pasar antes de que el dispositivo se elimine del grupo automáticamente. El intervalo de tiempo por defecto es de 60 días.

  Esta opción está activada de forma predeterminada.

- **Heredar del grupo primario**

  La configuración de la sección se heredará del grupo primario al que pertenezca el dispositivo cliente. Si esta opción está habilitada, los ajustes de la sección **Actividad de los dispositivos en la red** no se podrán modificar.

  Para que esta opción esté disponible, el grupo de administración debe tener un grupo primario.

  Esta opción está activada de forma predeterminada.

- **Forzar herencia en grupos secundarios**

  Los valores de configuración se propagarán a los grupos secundarios. Los ajustes correspondientes estarán bloqueados en las propiedades de esos grupos.

  Esta opción está deshabilitada de forma predeterminada.

5. Haga clic en **Aceptar**.

Se guardarán y aplicarán los cambios.

# Dejar de recibir las novedades de Kaspersky

En Kaspersky Security Center Web Console, la sección de anuncios de Kaspersky (**Supervisión e informes** → **Anuncios de Kaspersky**) lo mantiene informado al brindarle información relacionada con su versión de Kaspersky Security Center y las aplicaciones administradas instaladas en dispositivos administrados. Si ya no desea recibir novedades de Kaspersky, puede deshabilitar esta función.

Kaspersky publica dos clases de novedades: novedades sobre temas de seguridad y novedades con fines publicitarios. Puede deshabilitar cada clase de novedad por separado.

*Para dejar de recibir novedades sobre temas de seguridad:*

1. En el árbol de la consola, seleccione el Servidor de administración en el que desea deshabilitar los anuncios relacionados con la seguridad.
2. Haga clic derecho y seleccione **Propiedades** en el menú contextual que aparece.
3. En la ventana de propiedades del Servidor de administración que se abre, en la sección **Novedades de Kaspersky**, deshabilite la opción **Mostrar novedades de Kaspersky en Kaspersky Security Center Web Console**.
4. Haga clic en **Aceptar**.

Ya no recibirá novedades de Kaspersky.

Las novedades con fines publicitarios están deshabilitadas de forma predeterminada. Solo recibirá este tipo de novedades si ha habilitado Kaspersky Security Network (KSN). Puede deshabilitar este tipo de anuncios desactivando KSN.

# Ajuste de puntos de distribución y puertas de enlace de conexión

Una estructura de grupos de administración en Kaspersky Security Center realiza las funciones siguientes:

- Define el alcance de las directivas

  Existe otra forma de aplicar ajustes pertinentes en dispositivos: mediante el uso de *perfiles de directiva*. En este caso, el alcance de las directivas se establece a través de etiquetas, ubicaciones de dispositivos en unidades organizativas de Active Directory o membresías en grupos de seguridad de Active Directory.

- Define el alcance de las tareas de grupo

  Existe un modo de definir el alcance de las tareas de grupo que no depende de una jerarquía de grupos de administración: el uso de tareas para selecciones de dispositivos y de tareas para dispositivos específicos.

- Regula la capacidad de acceder a los distintos dispositivos, Servidores de administración secundarios y Servidores de administración virtuales

- Asigna puntos de distribución

Al momento de crear la estructura de grupos de administración, para que la asignación de puntos de distribución sea óptima, es necesario tener en cuenta la topología de la red de la organización. La distribución óptima de puntos de distribución le permite ahorrar tráfico en la red de la organización.

Dependiendo del organigrama de la organización y de la topología de la red, pueden aplicarse las siguientes configuraciones estándares a la estructura de grupos de administración:

- Oficina única
- Varias oficinas remotas pequeñas

Los dispositivos designados como puntos de distribución deben protegerse contra el acceso no autorizado por medios virtuales y físicos.

# Configuración estándar de puntos de distribución: oficina única

En una configuración estándar de "oficina única", todos los dispositivos se encuentran en la red de la organización y tienen la capacidad de "verse" los unos a los otros. La red de la organización puede constar de varias partes independientes (redes o segmentos de red) vinculadas por canales estrechos.

Los siguientes métodos pueden emplearse para armar la estructura de grupos de administración:

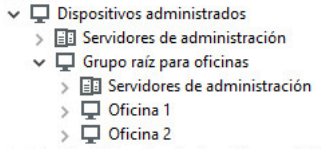
- Armar la estructura de grupos de administración tomando en cuenta la topología de la red. No es necesario que la estructura de grupos de administración refleje con absoluta precisión la topología de la red. Es suficiente con que haya coincidencia entre las partes independientes de la red y ciertos grupos de administración. Puede usar la asignación automática de puntos de distribución o asignarlos manualmente.

- Armar la estructura de grupos de administración sin tener en cuenta la topología de la red. En este caso, debe deshabilitar la asignación automática de puntos de distribución y luego asignar uno o varios dispositivos para que actúen como puntos de distribución para un grupo de administración original en cada una de las partes independientes de la red; por ejemplo, para el grupo **Dispositivos administrados**. Todos los puntos de distribución estarán al mismo nivel y presentarán el mismo alcance en todos los dispositivos en la red de la organización. En este caso, cada Agente de red se conectará al punto de distribución que tenga la ruta más corta. La ruta a un punto de distribución se puede determinar con la utilidad tracert.

# Configuración estándar de puntos de distribución: varias oficinas remotas pequeñas

Esta configuración estándar contempla la existencia de varias pequeñas oficinas remotas, que pueden comunicarse con una oficina central a través de Internet. Cada oficina remota está ubicada detrás de una pasarela NAT; debido a ello, las oficinas remotas están aisladas las unas de las otras y no se pueden conectar entre sí.

La configuración se debe ver reflejada en la estructura de grupos de administración: debe crearse un grupo de administración independiente para cada oficina remota (los grupos **Oficina 1** y **Oficina 2** en la siguiente imagen).




Oficinas remotas incluidas en la estructura de grupos de administración

Cada grupo de administración correspondiente a una oficina debe tener asignados uno o más puntos de distribución. Los puntos de distribución deben ser dispositivos que se encuentren en la oficina remota y deben tener una cantidad suficiente de espacio libre en disco. Los dispositivos incluidos en el grupo **Oficina 1** accederán a los puntos de distribución asignados al grupo de administración **Oficina 1**, por ejemplo.

Cuando hay usuarios que utilizan una computadora portátil para trabajar físicamente en más de una oficina, resulta necesario designar, junto con los puntos de distribución existentes, dos o más dispositivos en cada oficina remota para que actúen como puntos de distribución de un grupo de administración ubicado en un nivel superior (el grupo llamado **Grupo para oficinas** en la imagen anterior).

Ejemplo: Una computadora portátil incluida en el grupo de administración **Oficina 1** se traslada físicamente a la oficina que corresponde al grupo de administración **Oficina 2**. Luego del traslado, el Agente de red de la computadora portátil intenta acceder a los puntos de distribución asignados al grupo **Oficina 1**, pero esos puntos de distribución no están disponibles. Tras ello, el Agente de red intenta acceder a los puntos de distribución asignados al **Grupo para oficinas**. Como las oficinas remotas están aisladas entre sí, los intentos de acceder a los puntos de distribución asignados al grupo de administración **Grupo para oficinas** solo tendrán éxito cuando el Agente de red intente acceder a los puntos de distribución del grupo **Oficina 2**. Así, la computadora portátil permanecerá en el grupo de administración correspondiente a su oficina inicial, pero usará el punto de distribución de la oficina en la que se encuentre físicamente.

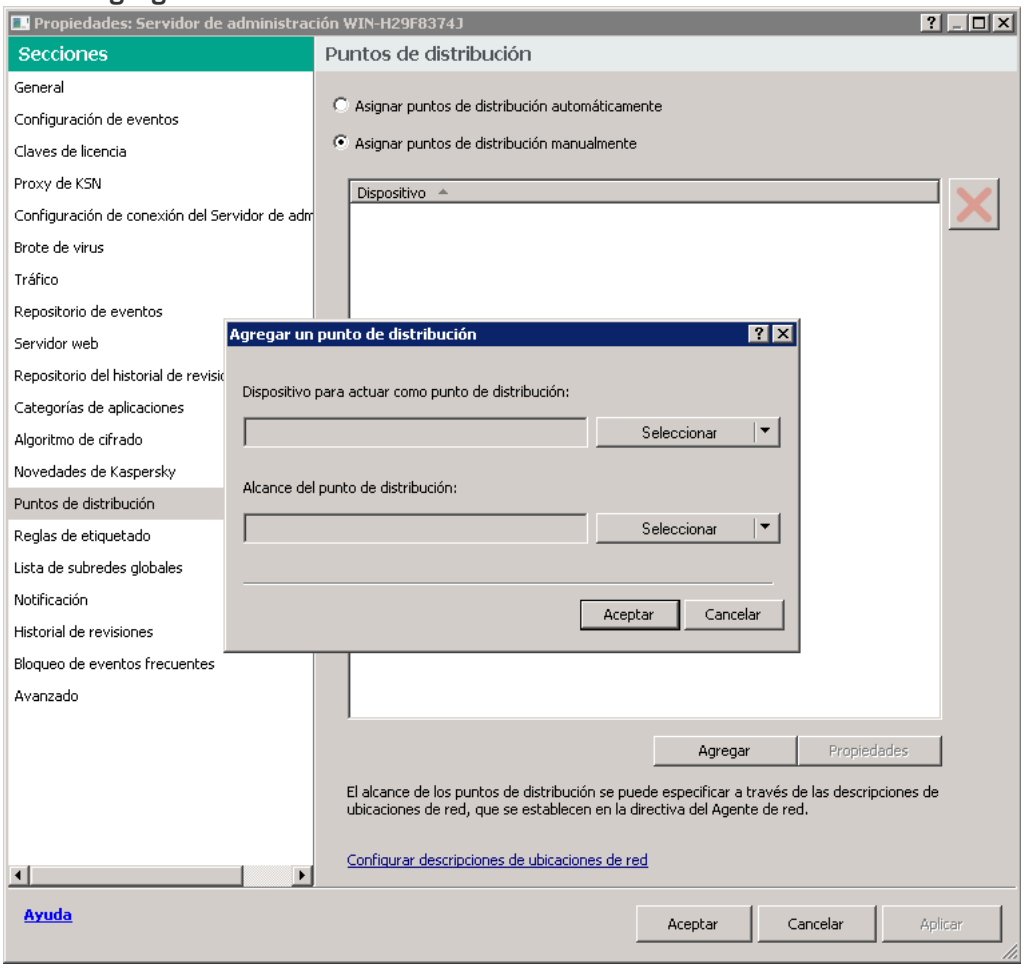
# Designación de un dispositivo administrado como un punto de distribución

Puede utilizar la Consola de administración para designar manualmente un dispositivo como punto de distribución para un grupo de administración y configurar dicho dispositivo como puerta de enlace de conexión.

*Para asignar un dispositivo como punto de distribución de un grupo de administración:*

1. En el árbol de consola, haga clic el nodo del **Servidor de administración**.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
3. En la ventana de propiedades del Servidor de administración, seleccione la sección **Puntos de distribución**.
4. En la parte derecha de la ventana, seleccione la opción **Asignar manualmente puntos de distribución**.

5. Haga clic en el botón **Agregar**.




Asignación manual de un punto de distribución

Se abre la ventana **Agregar un punto de distribución**.

6. En la ventana **Agregar un punto de distribución**, realice las siguientes acciones:

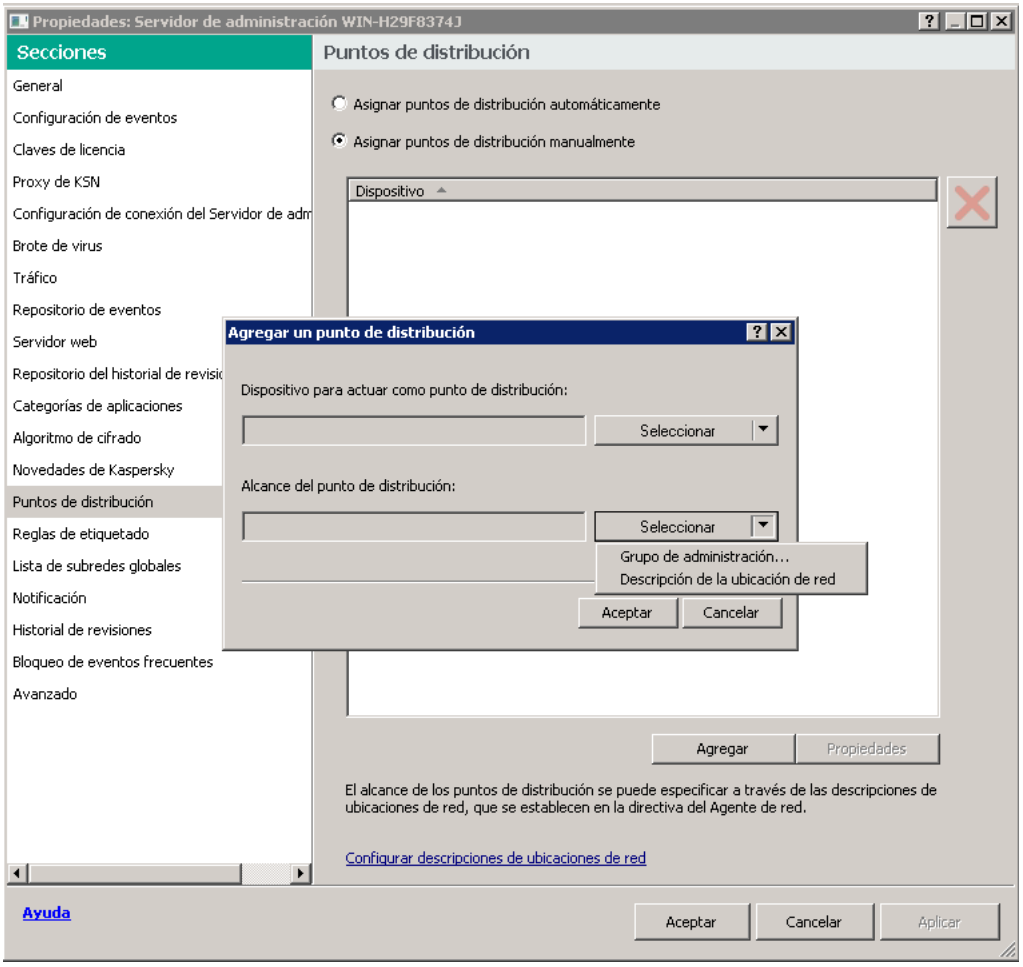
   a. Bajo **Dispositivo para actuar como punto de distribución**, busque el botón dividido **Seleccionar**, haga clic en la flecha descendente (▼) y elija la opción **Agregar dispositivo desde grupo**.

   b. En la ventana **Seleccionar los dispositivos** que se abre, seleccione el dispositivo que actuará como punto de distribución.

   c. Bajo **Alcance del punto de distribución**, busque el botón dividido **Seleccionar** y haga clic en la flecha descendente (▼).

   d. Indique los dispositivos específicos a los que el punto de distribución distribuirá las actualizaciones. Puede especificar un grupo de administración o una descripción de ubicación de red.

e. Haga clic en **Aceptar** para cerrar la ventana **Agregar un punto de distribución**.




Selección del alcance del punto de distribución

El punto de distribución agregado aparecerá en la lista de puntos de distribución, en la sección **Puntos de distribución**.

El primer dispositivo que tenga instalado el Agente de red y que se conecte al Servidor de administración virtual se asignará automáticamente para que funcione como el punto de distribución y se configurará como la puerta de enlace de conexión.

# Conexión de un dispositivo Linux como una puerta de enlace en la zona desmilitarizada

*Para conectar un dispositivo Linux como una puerta de enlace en la zona desmilitarizada (DMZ), realice lo siguiente:*

1. Descargue e instale el Agente de red en el dispositivo Linux.

2. Ejecute el script posterior a la instalación y siga el Asistente para establecer la configuración del entorno local. En el símbolo del sistema, ejecute el siguiente comando:
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. Cuando se le pregunte, en uno de los pasos, por el modo del Agente de red, elija la opción **Usar como puerta de enlace de conexión**.

4. En la Consola de administración basada en MMC, abra el menú contextual del Servidor de administración y seleccione **Propiedades**.

5. En la ventana de propiedades del Servidor de administración que se abre, seleccione la sección **Puntos de distribución**.

6. Cuando se abra la ventana **Puntos de distribución**, haga lo siguiente en la parte derecha de la misma:

   a. Seleccione la opción **Asignar manualmente puntos de distribución**.

   b. Haga clic en el botón **Agregar**.

   Se abre la ventana **Agregar un punto de distribución**.

7. En la ventana **Agregar un punto de distribución**, realice las siguientes acciones:

   a. En **Dispositivo para actuar como punto de distribución**, haga clic en la flecha descendente ( ) en el botón de expansión **Seleccionar** y seleccione la opción **Agregar la puerta de enlace de conexión en DMZ por dirección**.

   b. Bajo **Alcance del punto de distribución**, busque el botón dividido **Seleccionar** y haga clic en la flecha descendente ( ).

   c. Indique los dispositivos específicos a los que el punto de distribución distribuirá las actualizaciones. Puede especificar un grupo de administración.

   d. Haga clic en **Aceptar** para cerrar la ventana **Agregar un punto de distribución**.

8. El punto de distribución agregado aparecerá en la lista de puntos de distribución, en la sección **Puntos de distribución**.

9. Ejecute la utilidad klnagchk para comprobar que la conexión a Kaspersky Security Center se haya configurado correctamente. En la línea de comandos, ejecute lo siguiente:
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```

10. En el menú principal, vaya a Kaspersky Security Center y descubra el dispositivo.

11. En la ventana que se abre, haga clic en el <nombre del dispositivo>.

12. En la lista desplegable, haga clic en el vínculo **Mover a un grupo**.

13. En la ventana **Seleccionar grupo** que se abre, haga clic en el vínculo **Puntos de distribución**.

14. Haga clic en **Aceptar**.

15. Ejecute el siguiente comando para reiniciar el servicio del Agente de red en el cliente Linux:
    ```
    $ sudo /opt/kaspersky/klnagent64/bin/klnagchk -restart
    ```

Se completa la conexión del dispositivo Linux como una puerta de enlace en la DMZ.

Después, puede conectar un dispositivo Linux al Servidor de administración a través de una puerta de enlace de conexión. No realice el procedimiento que se describe en esta sección si aún no ha concluido el escenario de instalación principal.

# Conexión de un dispositivo Linux al Servidor de administración a través de una puerta de enlace de conexión

Una puerta de enlace de conexión le permite conectar dispositivos cliente desde la zona desmilitarizada (DMZ) al Servidor de administración. Los dispositivos basados en Windows y Linux pueden actuar como una puerta de enlace de conexión. Tras conectar y configurar la puerta de enlace de conexión, puede usarla para conectar dispositivos Linux al Servidor de administración. No realice el procedimiento que se describe en esta sección si aún no ha concluido el escenario de instalación principal.

*Para conectar un dispositivo Linux al Servidor de administración a través de una puerta de enlace de conexión, realice las siguientes acciones en este dispositivo:*

1. Descargue e instale el Agente de red en el dispositivo Linux.

2. Ejecute el script de postinstalación del Agente de red. Para ello, introduzca el siguiente comando en una terminal:
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. Cuando se le pregunte, en uno de los pasos, por el modo del Agente de red, elija la opción **Conectarse al servidor mediante una puerta de enlace de conexión** e ingrese la dirección de la puerta de conexión.

4. Compruebe la conexión con Kaspersky Security Center y la puerta de enlace, usando el siguiente comando en la línea de comandos:
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```
   Se muestra la dirección de la puerta de enlace de conexión en la salida.

Se completó la conexión de un dispositivo Linux al Servidor de administración a través de una puerta de enlace de conexión. Puede utilizar este dispositivo para actualizar la distribución, para instalar aplicaciones de forma remota y para recuperar información sobre dispositivos en red.

# Agregar una puerta de enlace de conexión ubicada en una DMZ como punto de distribución

Una puerta de enlace de conexión no busca conectarse con el Servidor de administración; por el contrario, espera que el Servidor de administración se conecte con ella. Es por esto que, si instala una puerta de enlace de conexión en un dispositivo ubicado en su DMZ, el Servidor de administración no incluirá al dispositivo entre los dispositivos administrados. El problema puede resolverse con un procedimiento especial, que obliga al Servidor de administración a conectarse con la puerta de enlace de conexión.

*Para agregar una puerta de enlace de conexión como punto de distribución:*

1. En el árbol de consola, haga clic el nodo del **Servidor de administración**.

2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.

3. En la ventana de propiedades del Servidor de administración, seleccione la sección **Puntos de distribución**.

4. En la parte derecha de la ventana, seleccione la opción **Asignar manualmente puntos de distribución**.

5. Haga clic en el botón **Agregar**.

   Se abre la ventana **Agregar un punto de distribución**.

6. En la ventana **Agregar un punto de distribución**, realice las siguientes acciones:

   a. En **Dispositivo para actuar como punto de distribución**, busque el botón dividido **Seleccionar**, haga clic en la flecha descendente (▾) y, luego, elija la opción **Agregar puerta de enlace de conexión en la DMZ por dirección**.

   b. En la ventana **Ingresar dirección de la puerta de enlace de conexión** que se abre, introduzca la dirección IP de la puerta de enlace de conexión (o introduzca el nombre si la puerta de enlace de conexión es accesible por su nombre).

   c. Bajo **Alcance del punto de distribución**, busque el botón dividido **Seleccionar** y haga clic en la flecha descendente (▾).

   d. Indique los dispositivos específicos a los que el punto de distribución distribuirá las actualizaciones. Puede especificar un grupo de administración o una descripción de ubicación de red.

      Recomendamos utilizar un grupo independiente para los dispositivos administrados externos.

Tras realizar estas acciones, encontrará una nueva entrada en la lista de puntos de distribución, con el nombre **Entrada temporal para puerta de enlace de conexión**.

El Servidor de administración casi inmediatamente intenta conectarse a la puerta de enlace de conexión en la dirección que especificó. Si tiene éxito, el nombre de la entrada cambia al nombre del dispositivo de puerta de enlace de conexión. El proceso puede tomar hasta cinco minutos.

Mientras que la entrada temporal para la puerta de enlace de conexión se convierte en una entrada con nombre, la puerta de enlace de conexión también aparece en el grupo **Dispositivos no asignados**.

Para agregar una puerta de enlace de conexión a una red ya configurada, vuelva a instalar el Agente de red en los dispositivos que desea conectar a la puerta de enlace de la conexión recién agregada.

# Asignar puntos de distribución automáticamente

Recomendamos que asigne puntos de distribución automáticamente. Kaspersky Security Center seleccionará por sí mismo qué dispositivos deben tener asignados puntos de distribución.

*Para asignar puntos de distribución automáticamente:*

1. Abra la ventana principal de la aplicación.

2. En el árbol de la consola, seleccione el nodo con el nombre del Servidor de administración para el que desea asignar puntos de distribución automáticamente.

3. En el menú contextual del Servidor de administración, haga clic en **Propiedades**.

4. En la ventana de propiedades del Servidor de administración, en el panel **Secciones**, seleccione **Puntos de distribución**.

5. En la parte derecha de la ventana, seleccione la opción **Asignar puntos de distribución automáticamente**.

Si la asignación automática de dispositivos como puntos de distribución está habilitada, no puede configurar los puntos de distribución manualmente ni editar la lista de puntos de distribución.

6. Haga clic en **Aceptar**.

El Servidor de administración asigna y configura los puntos de distribución automáticamente.

# Acerca de la instalación local del Agente de red en un dispositivo seleccionado como punto de distribución

Para permitir que el dispositivo seleccionado como punto de distribución se comunique directamente con el Servidor de administración virtual a fin de funcionar como puerta de enlace de conexión, el Agente de red se debe instalar localmente en ese dispositivo.

El procedimiento de instalación local del Agente de red en el dispositivo definido como punto de distribución es igual al de instalación local del Agente de red en cualquier dispositivo de red.

El dispositivo seleccionado para funcionar como punto de distribución debe cumplir las siguientes condiciones:

- Durante la instalación local del Agente de red, especifique la dirección de un Servidor de administración virtual que administra el dispositivo en el campo **Dirección del servidor**, en la ventana **Servidor de administración** del Asistente de instalación. Puede usar la dirección IP o el nombre del dispositivo en la red de Windows.

  El siguiente formato se utiliza para la dirección del Servidor de administración virtual: <Dirección completa del Servidor de administración físico al que se subordina el Servidor virtual>/<Nombre del Servidor de administración virtual>.

- Para que pueda funcionar como puerta de enlace de conexión, abra todos los puertos del dispositivo que son necesarios para la comunicación con el Servidor de administración.

Después de que el Agente de red con la configuración especificada se instala en un dispositivo, Kaspersky Security Center realiza las siguientes acciones de manera automática:

- Incluye el dispositivo en el grupo **Dispositivos administrados** del Servidor de administración virtual.
- Designa este dispositivo como el punto de distribución del grupo **Dispositivos administrados** del Servidor de administración virtual.

Es necesario y suficiente instalar el Agente de red localmente en el dispositivo que se asignó como punto de distribución para el grupo **Dispositivos administrados** en la red de la organización. Puede instalar el Agente de red de manera remota en los dispositivos que funcionan como puntos de distribución en los grupos de administración anidados. Para ello, use el punto de distribución del grupo **Dispositivos administrados** como puerta de enlace de conexión.

# Acerca del uso de un punto de distribución como puerta de enlace de conexión

Si el Servidor de administración se encuentra fuera de la zona desmilitarizada (DMZ), los Agentes de red de esta zona no pueden conectarse al Servidor de administración.

Al conectar el Servidor de administración con los Agentes de red, puede usar un punto de distribución como puerta de enlace de conexión. El punto de distribución abre un puerto al Servidor de administración para que se cree la conexión. Cuando se inicia el Servidor de administración, se conecta a ese punto de distribución y mantiene esta conexión durante toda la sesión.

Al recibir una señal del Servidor de administración, el punto de distribución envía una señal UDP a los Agentes de red para permitir la conexión al Servidor de administración. Cuando los Agentes de red reciben esa señal, se conectan al punto de distribución, que transfiere información entre los Agentes de red y el Servidor de administración. El intercambio de información puede ocurrir a través de una red IPv4 o IPv6.

Recomendamos que use un dispositivo asignado especialmente como puerta de enlace de conexión y abarque un máximo de 10 000 dispositivos cliente (entre ellos dispositivos móviles) con esta puerta de enlace de conexión.

*Para agregar una puerta de enlace de conexión a una red ya configurada:*

1. Instale el Agente de red en el modo de puerta de enlace de conexión.
2. Vuelva a instalar el Agente de red en los dispositivos que desee conectar a la puerta de enlace de conexión recién agregada.

# Agregar rangos de IP a la lista de rangos sondeados por un punto de distribución

Puede agregar un rango de IP a la lista de rangos sondeados por un punto de distribución.

*Para agregar un rango de IP a la lista de rangos sondeados:*

1. En el árbol de consola, haga clic el nodo del **Servidor de administración**.
2. En el menú contextual del nodo, seleccione **Propiedades**.
3. En la ventana de propiedades del Servidor de administración que se abre, seleccione la sección **Puntos de distribución**.
4. En la lista, seleccione el punto de distribución necesario y, luego, haga clic en **Propiedades**.
5. En la ventana de propiedades del punto de distribución que se abre, en el panel izquierdo **Secciones**, seleccione **Descubrimiento de dispositivos → Intervalos IP**.
6. Seleccione la casilla **Habilitar el sondeo del rango**.

7. Haga clic en el botón **Agregar**.

   El botón **Agregar** está activo solo si selecciona la casilla de verificación **Habilitar el sondeo del rango**.

   Se abre la ventana del **Intervalo IP**.

8. En la ventana de **Intervalo IP**, introduzca el nombre del nuevo rango de IP (el nombre predeterminado es Nuevo rango).

9. Haga clic en el botón **Agregar**.

10. Realice una de las siguientes acciones:

    - Especifique el rango de IP utilizando las direcciones IP de iniciales y finales.
    - Especifique el rango de IP utilizando la dirección y la máscara de subred.
    - Haga clic en **Examinar** y añada una subred de la lista global de subredes.

11. Haga clic en **Aceptar**.

12. Haga clic en **Aceptar** para añadir el nuevo rango con el nombre especificado.

    El nuevo rango aparecerá en la lista de rangos sondeados.

# Uso de un punto de distribución como servidor push

En Kaspersky Security Center, un punto de distribución puede funcionar como servidor push para los dispositivos administrados a través del protocolo móvil y para los dispositivos administrados por el Agente de red. Por ejemplo, se debe habilitar un servidor push si quiere poder forzar la sincronización de los dispositivos KasperskyOS con el Servidor de administración. Un servidor push tiene el mismo alcance de los dispositivos administrados que el punto de distribución en el que se habilitar el servidor push. Si tiene varios puntos de distribución asignados para el mismo grupo de administración, puede habilitar el servidor push en cada uno de los puntos de distribución. En este caso, el Servidor de administración equilibra la carga entre los puntos de distribución.

Un servidor push soporta la carga de hasta 50 000 conexiones simultáneas.

Puede utilizar puntos de distribución como servidores push para asegurarse de que haya una conectividad continua entre un dispositivo administrado y el Servidor de administración. Se necesita conectividad continua para algunas operaciones, como ejecutar y detener tareas locales, recibir estadísticas para una aplicación administrada o crear un túnel. Si utiliza un punto de distribución como servidor push, no es necesario utilizar la opción **No desconectar del Servidor de administración** en dispositivos administrados ni enviar paquetes al puerto UDP del Agente de red.

*Para usar un punto de distribución como servidor push:*

1. En el árbol de consola, haga clic el nodo del **Servidor de administración**.

2. En el menú contextual del nodo, seleccione **Propiedades**.

3. En la ventana de propiedades del Servidor de administración que se abre, seleccione la sección **Puntos de distribución**.

4. En la lista, seleccione el punto de distribución necesario y, luego, haga clic en **Propiedades**.

5. En la ventana de propiedades del punto de distribución que se abre, en la sección **General** del panel izquierdo **Secciones**, seleccione la opción **Utilice este punto de distribución como servidor push**.

6. Especifique el número de puerto del servidor push, es decir, el puerto del punto de distribución que los dispositivos cliente utilizarán para conectarse.

   De manera predeterminada, se utiliza el puerto 13295.

7. Haga clic en el botón **Aceptar** para salir de la ventana de propiedades del punto de distribución.

8. Abra la ventana de configuración de la directiva del Agente de red.

9. En la sección **Conectividad**, vaya a la subsección **Red**.

10. En la subsección **Red**, seleccione la opción **Utilice el punto de distribución para forzar la conexión con el Servidor de administración**.

11. Haga clic en el botón **Aceptar** para salir de la ventana.

El punto de distribución funcionará como servidor push. Ya puede enviar notificaciones push a los dispositivos cliente.

Si administra los dispositivos con KasperskyOS instalado, o tiene pensado hacerlo, debe utilizar un punto de distribución como servidor push. También puede utilizar un punto de distribución como servidor push si desea enviar notificaciones push a los dispositivos cliente.

# Otro trabajo de rutina

Esta sección proporciona recomendaciones sobre el trabajo rutinario con Kaspersky Security Center.

# Administración de los Servidores de administración

Esta sección proporciona información sobre cómo trabajar con los Servidores de administración y cómo configurarlos.

## Creación de una jerarquía de servidores de administración: agregar un Servidor de administración secundario

Puede agregar un Servidor de administración como Servidor de administración secundario, estableciendo así una jerarquía "principal/secundario". Es posible agregar un Servidor de administración secundario sin importar si el Servidor de administración que tiene la intención de usar como secundario está disponible para conectarse a través de la Consola de administración.

Al combinar dos Servidores de administración en una jerarquía, asegúrese de que el puerto 13291 esté accesible en ambos Servidores de administración. El Puerto 13291 se requiere para recibir conexiones de la Consola de administración al Servidor de administración.

## Conexión de un Servidor de administración como secundario en referencia al Servidor de administración principal

Puede agregar un Servidor de administración como secundario conectándolo al Servidor de administración principal a través del puerto 13000. Necesitará un dispositivo que tenga instalada la Consola de administración desde la cual se pueda acceder al puerto TCP 13291 en ambos Servidores de administración: el supuesto Servidor de administración principal y el supuesto Servidor de administración secundario.

*Para agregar como secundario un Servidor de administración que esté disponible para conectarse a través de la Consola de administración:*

1. Asegúrese de que el puerto 13000 del supuesto Servidor de administración principal esté disponible para la recepción de conexiones desde los Servidores de administración secundarios.

2. Use la Consola de administración para conectarse al supuesto Servidor de administración principal.

3. Seleccione el grupo de administración al que desea agregar el Servidor de administración secundario.

4. En el espacio de trabajo del nodo del grupo **Servidores de administración** seleccionado, haga clic en el enlace **Agregar un Servidor de administración secundario**.

   Se inicia el Asistente para agregar un Servidor de administración secundario.

5. En el primer paso del Asistente (entrada de la dirección del Servidor de administración que se agrega al grupo), escriba el nombre de la red del supuesto Servidor de administración secundario.

6. Siga las instrucciones del asistente.

Así se constituye la jerarquía "principal/secundario". El Servidor de administración principal recibirá la conexión del Servidor de administración secundario.

Si no dispone de un dispositivo que tenga instalada la Consola de administración desde la cual se pueda acceder al puerto TCP 13291 en ambos Servidores de administración (si, por ejemplo, el supuesto Servidor de administración secundario se encuentra en una oficina remota y el administrador del sistema de esa oficina no puede abrir el acceso a Internet para el puerto 13291 por razones de seguridad), de todos modos podrá agregar un Servidor de administración secundario.

*Para agregar como secundario un Servidor de administración que no esté disponible para la conexión a través de la Consola de administración:*

1. Asegúrese de que el puerto 13000 del supuesto Servidor de administración principal esté disponible para la conexión de los Servidores de administración secundarios.

2. Guarde el archivo de certificado del supuesto Servidor de administración principal en un dispositivo externo (por ejemplo, una unidad flash) o envíelo al administrador del sistema de la oficina remota en la que se encuentre el Servidor de administración.

   El archivo del certificado del Servidor de administración está en el mismo Servidor de administración, en %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

3. Escriba el archivo del certificado del supuesto Servidor de administración secundario y guárdelo en un dispositivo externo, como una unidad flash. Si el supuesto Servidor de administración secundario se localiza en una oficina remota, póngase en contacto con el administrador del sistema de esa oficina para solicitarle que le envíe el certificado.

   El archivo del certificado del Servidor de administración está en el mismo Servidor de administración, en %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

4. Use la Consola de administración para conectarse al supuesto Servidor de administración principal.

5. Seleccione el grupo de administración al que desea agregar el Servidor de administración secundario.

6. En el espacio de trabajo de este nodo **Servidores de administración**, haga clic en el enlace **Agregar un Servidor de administración secundario**.

   Se inicia el Asistente para agregar un Servidor de administración secundario.

7. En el primer paso del Asistente (entrada de la dirección), deje el campo **Dirección del Servidor de administración secundario (opcional)** en blanco.

8. En la ventana **Archivo del certificado del Servidor de administración secundario**, haga clic en el botón **Examinar** y seleccione el archivo de certificado del Servidor de administración secundario que guardó.

9. Cuando el Asistente se haya completado, use otra instancia de la Consola de administración para conectarse con el supuesto Servidor de administración secundario. Si este Servidor de administración se encuentra en una oficina remota, póngase en contacto con el administrador del sistema de esa oficina para solicitarle que se conecte al supuesto Servidor de administración secundario y realice los pasos adicionales.

10. En el menú contextual del nodo **Servidor de administración**, seleccione **Propiedades**.

11. En las propiedades del Servidor de administración, vaya a la sección **Avanzado** y luego a la subsección **Jerarquía de servidores de administración**.

12. Marque la casilla **Este Servidor de administración es un servidor secundario en la jerarquía**.

    Los campos de entrada están disponibles para el ingreso y modificación de datos.

13. En el campo **Dirección del Servidor de administración principal**, ingrese el nombre de red del supuesto Servidor de administración principal.

14. Seleccione el archivo guardado anteriormente con el certificado del supuesto Servidor de administración principal haciendo clic en el botón **Examinar**.

15. Haga clic en **Aceptar**.

Así se constituye la jerarquía "principal/secundario". Puede conectarse al Servidor de administración secundario a través de la Consola de administración. El Servidor de administración principal recibirá la conexión del Servidor de administración secundario.

## Conexión del Servidor de administración principal a un Servidor de administración secundario

Puede agregar un nuevo Servidor de administración como secundario para que el Servidor de administración principal se conecte al Servidor de administración secundario a través del puerto 13000. Esto es recomendable si, por ejemplo, coloca un Servidor de administración secundario en la "zona desmilitarizada" (DMZ).

Necesitará un dispositivo que tenga instalada la Consola de administración desde la cual se pueda acceder al puerto TCP 13291 en ambos Servidores de administración: el supuesto Servidor de administración principal y el supuesto Servidor de administración secundario.

*Para agregar un nuevo Servidor de administración como secundario y conectar el Servidor de administración principal a través del puerto 13000:*

1. Asegúrese de que el puerto 13000 del supuesto Servidor de administración secundario esté disponible para la recepción de conexiones del Servidor de administración principal.
2. Use la Consola de administración para conectarse al supuesto Servidor de administración principal.
3. Seleccione el grupo de administración al que desea agregar el Servidor de administración secundario.
4. En el espacio de trabajo del nodo del grupo de administración **Servidores de administración** relevante, haga clic en el enlace **Agregar un Servidor de administración secundario**.

   Se inicia el Asistente para agregar un Servidor de administración secundario.
5. En el primer paso del Asistente (entrada de la dirección del Servidor de administración que se agregará al grupo), ingrese el nombre de red del supuesto Servidor de administración secundario y seleccione la casilla **Conectar el Servidor de administración principal a un Servidor de administración secundario en DMZ**.
6. Si se conecta al supuesto Servidor de administración secundario con un servidor proxy, en el primer paso del Asistente, seleccione la casilla **Usar servidor proxy** y especifique la configuración de conexión.
7. Siga las instrucciones del asistente.

Se crea la jerarquía de Servidores de administración. El Servidor de administración secundario recibirá la conexión del Servidor de administración principal.

## Conexión a un Servidor de administración y alternancia entre Servidores de administración

Una vez iniciado, Kaspersky Security Center intenta conectarse a un Servidor de administración. Si existen varios Servidores de administración disponibles en la red, la aplicación solicita el Servidor al que se conectó durante la sesión anterior de Kaspersky Security Center.

> La primera vez que se inicia la aplicación después de la instalación, intenta conectarse al Servidor de administración especificado durante la instalación de Kaspersky Security Center.

Una vez establecida la conexión con un Servidor de administración, el árbol de carpetas de ese Servidor se muestra en el árbol de consola.

Si se agregaron varios Servidores de administración al árbol de consola, puede cambiar entre esos servidores.

La Consola de administración es necesaria para trabajar con cada Servidor de administración. Antes de la primera conexión a un nuevo Servidor de administración, asegúrese de que el puerto 13291, que recibe conexiones desde la Consola de administración, esté abierto, así como todos los puertos restantes necesarios para la comunicación entre el Servidor de administración y otros componentes de Kaspersky Security Center.

*Para conectarse a otro Servidor de administración:*

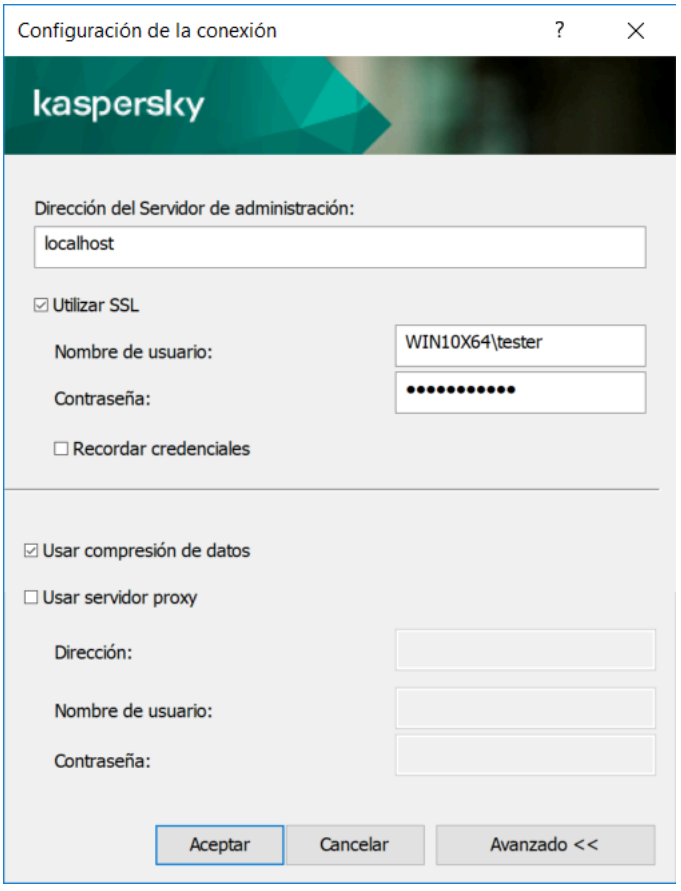
1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el menú contextual del nodo, seleccione **Conectarse al Servidor de administración**.

3. En la ventana **Configuración de la conexión** que se abre, especifique en el campo **Dirección del Servidor de administración** el nombre del Servidor de administración al que desea conectarse. Puede especificar una dirección IP o el nombre de un dispositivo de una red de Windows como nombre del Servidor de administración. Puede hacer clic en el botón **Avanzado** para configurar la conexión al Servidor de administración (vea la siguiente figura).

   Para conectarse al Servidor de administración mediante un puerto diferente del predeterminado, ingrese un valor en el campo **Dirección del Servidor de administración** con el formato <Nombre del Servidor de administración>:<Puerto>.

   Para conectarse a un Servidor de administración virtual, ingrese un valor en el campo **Dirección del Servidor de administración** en formato <Dirección del Servidor de administración>/<nombre del servidor virtual>.

   > Los usuarios que no tienen derechos de **lectura** no tendrán acceso al Servidor de administración.




Conexión al Servidor de administración

4. Haga clic en el botón **Aceptar** para completar el cambio entre Servidores.

   Una vez que el Servidor de administración está conectado, se actualiza el árbol de carpeta del nodo correspondiente en el árbol de consola.

## Permisos de acceso al Servidor de administración y sus objetos

Los grupos **KLAdmins** y **KLOperators** se crean automáticamente durante la instalación de Kaspersky Security Center. A estos grupos se les otorgan permisos para conectarse al Servidor de administración y procesar los objetos de este.

Según el tipo de cuenta que se use para instalar Kaspersky Security Center, los grupos **KLAdmins** y **KLOperators** se crean de la siguiente manera:

- Si la aplicación se instala con una cuenta de usuario incluida en un dominio, los grupos se crean en el dominio que incluye el Servidor de administración y en el propio Servidor de administración.
- Si la aplicación se instala con una cuenta de sistema, los grupos se crean solo en el Servidor de administración.

Puede ver los grupos **KLAdmins** y **KLOperators**, y modificar los privilegios de acceso de los usuarios que pertenecen a los grupos **KLAdmins** y **KLOperators** utilizando las herramientas administrativas estándar del sistema operativo.

El grupo **KLAdmins** tiene todos los permisos de acceso; el grupo **KLOperators** únicamente tiene permisos de Lectura y Ejecución. Los permisos otorgados al grupo **KLAdmins** están bloqueados.

Los usuarios que pertenecen al grupo **KLAdmins** se denominan *administradores de Kaspersky Security Center*; los usuarios del grupo **KLOperators** se denominan *operadores de Kaspersky Security Center*.

Los derechos de administrador de Kaspersky Security Center no solo se otorgan a los usuarios incluidos en el grupo **KLAdmins**, sino que también se otorgan a los administradores locales de los dispositivos en los que está instalado el Servidor de administración.

Puede excluir a los administradores locales de la lista de usuarios que poseen permisos de administrador de Kaspersky Security Center.

Todas las operaciones iniciadas por los administradores de Kaspersky Security Center serán realizadas usando los permisos de la cuenta del Servidor de administración.

Se puede crear un grupo individual **KLAdmins** para cada Servidor de administración desde la red; el grupo tendrá los permisos necesarios para ese Servidor de administración únicamente.

Si dispositivos que pertenecen al mismo dominio están incluidos dentro de grupos de administración de diferentes Servidores de administración, el administrador del dominio es un administrador de Kaspersky Security Center para todos los grupos. El grupo **KLAdmins** es el mismo para estos grupos de administración; éste se crea durante la instalación del primer Servidor de administración. Todas las operaciones iniciadas por el administrador de Kaspersky Security Center se realizan utilizando los permisos de la cuenta del Servidor de administración para el cual se iniciaron dichas operaciones.

Una vez instalada la aplicación, un administrador de Kaspersky Security Center puede hacer lo siguiente:

- Modificar los permisos concedidos a los grupos **KLOperators**.
- Conceder derechos (para acceder a la funcionalidad de Kaspersky Security Center) a otros grupos de seguridad y usuarios individuales registrados en la estación de trabajo del administrador.
- Asignar derechos de acceso a los usuarios en cada grupo de administración.

El administrador de Kaspersky Security Center puede asignar permisos de acceso a cada grupo de administración o a otros objetos del Servidor de administración, en la sección **Seguridad** de la ventana de propiedades del objeto seleccionado.

Puede realizar un seguimiento de la actividad de usuario mediante los registros de eventos en el funcionamiento del Servidor de administración. Los archivos del evento se muestran en el nodo **Servidor de administración** en la pestaña **Eventos**. Estos eventos tienen el nivel de importancia **Eventos informativos** y comienzan con la palabra **Auditoría**.

# Condiciones de conexión a un Servidor de administración a través de Internet

Si un Servidor de administración está ubicado fuera de una red corporativa, los dispositivos cliente se conectarán a este a través de Internet.

Para que los dispositivos se conecten a un Servidor de administración a través de Internet, se deben cumplir las siguientes condiciones:

- El Servidor de administración remota debe tener una dirección IP externa y el puerto entrante 13000 debe permanecer abierto (para la conexión de los agentes de red). Le recomendamos que también abra el puerto UDP 13000 (para recibir notificaciones de apagado del dispositivo).
- Primero deben instalarse los Agentes de red en los dispositivos.
- Al instalar el Agente de red en dispositivos, debe especificar la dirección IP externa del Servidor de administración remoto. Si se utiliza un paquete de instalación para la instalación, la dirección IP externa se debe especificar manualmente en las propiedades de este paquete, en la sección **Configuración**.
- Para usar el Servidor de administración remoto con el fin de administrar las aplicaciones y tareas de un dispositivo, en la ventana de propiedades de ese dispositivo, en la sección **General**, seleccione la casilla **No desconectar del Servidor de administración**. Una vez que la casilla está seleccionada, espere a que el Servidor de administración esté sincronizado con el dispositivo remoto. El número de dispositivos cliente que mantienen una conexión continua con un Servidor de administración remoto no puede superar los 300.

Para acelerar el rendimiento de las tareas generadas por un Servidor de administración remoto, puede abrir el puerto 15000 en un dispositivo. En este caso, para ejecutar una tarea, el Servidor de administración envía un paquete especial al Agente de red a través del puerto 15000 sin esperar a que se complete la sincronización con el dispositivo.

# Conexión cifrada con un Servidor de administración

El intercambio de datos entre los dispositivos cliente y el Servidor de administración, así como la conexión de la Consola de administración al Servidor de administración, puede realizarse mediante el protocolo TLS (Transport Layer Security). El protocolo TLS puede identificar las partes que interactúan, cifrar los datos que se transfieren y protegerlos de las modificaciones durante la transferencia. El protocolo TLS usa claves públicas para autenticar las partes que interactúan y cifrar datos.

## Autenticación del Servidor de administración cuando un dispositivo se conecta

Cuando un dispositivo cliente se conecta al Servidor de administración por primera vez, el Agente de red del dispositivo descarga una copia del certificado del Servidor de administración y lo almacena localmente.

> Si instala el Agente de red en un dispositivo localmente, puede seleccionar el certificado del Servidor de administración manualmente.

La copia descargada del certificado se utiliza para verificar los permisos del Servidor de administración durante las siguientes conexiones.

Durante futuras sesiones, el Agente de red solicita el certificado del Servidor de administración en cada conexión del dispositivo al Servidor y lo compara con la copia local. Si las copias no coinciden, el dispositivo no podrá acceder al Servidor de administración.

### Autenticación del Servidor de administración durante la conexión de la Consola de administración

Durante la primera conexión al Servidor de administración, la Consola de administración solicita el certificado del Servidor de administración y lo guarda localmente, en la estación de trabajo del administrador. Después de ello, cada vez que la Consola de administración intenta conectarse con este Servidor de administración, este es identificado a partir de la copia del certificado.

Si el certificado del Servidor de administración no coincide con la copia almacenada en la estación de trabajo del administrador, la Consola de administración le pedirá que confirme la conexión al Servidor de administración con el nombre especificado y descargará un nuevo certificado. Una vez establecida la conexión, la Consola de administración guarda una copia del nuevo certificado del Servidor de administración, que será utilizada para identificar al Servidor en el futuro.

## Configuración de una lista de admitidos de direcciones IP para conectarse al Servidor de administración

De forma predeterminada, para iniciar sesión en Kaspersky Security Center, se puede utilizar cualquier dispositivo que permita abrir Kaspersky Security Center 14 Web Console (en adelante, Web Console) o la Consola de administración basada en MMC. Si lo desea, puede hacer que el Servidor de administración únicamente acepte conexiones de dispositivos que tengan una dirección IP permitida. Con ello, si un intruso averigua los datos de una cuenta de Kaspersky Security Center, no podrá iniciar sesión en Kaspersky Security Center porque la dirección IP de su dispositivo no estará en la lista de direcciones permitidas.

El control de dirección IP se realiza cuando el usuario inicia sesión en Kaspersky Security Center o ejecuta una aplicación que interactúa con el Servidor de administración a través de la interfaz OpenAPI de Kaspersky Security Center. En este momento, el dispositivo de un usuario intenta establecer una conexión con el Servidor de administración. Si la dirección IP del dispositivo no está en la lista de direcciones permitidas, ocurre un error de autenticación y el evento KLAUD_EV_SERVERCONNECT indica que no se estableció conexión con el Servidor de administración.

### Requisitos para la lista de direcciones IP permitidas

Las direcciones IP se controlan solo cuando las siguientes aplicaciones intentan conectarse al Servidor de administración:

- Servidor de Web Console

  Si normalmente inicia sesión en Web Console desde un dispositivo diferente del que tiene instalado el Servidor de Web Console, puede usar las herramientas de su sistema operativo para configurar un firewall en el dispositivo que tenga instalado el Servidor de Web Console. El firewall puede ayudar a impedir que los intrusos inicien sesión en Web Console.

- Consola de administración

- Aplicaciones que interactúan con el Servidor de administración a través de objetos de automatización de klakaut
- Aplicaciones que interactúan con el Servidor de administración a través de OpenAPI, como Kaspersky Anti Targeted Attack Platform o Kaspersky Security for Virtualization

Por consiguiente, debe especificar las direcciones de todo dispositivo que tenga instalada una de las aplicaciones anteriores.

La lista puede contener direcciones IPv4 e IPv6. No puede contener intervalos de direcciones IP.

## Cómo definir una lista de direcciones IP permitidas

Si es la primera vez que crea una lista de direcciones permitidas, siga estas instrucciones.

*Para definir la lista de direcciones IP que podrán iniciar sesión en Kaspersky Security Center:*

1. En el dispositivo en el que se encuentre instalado el Servidor de administración, abra el símbolo del sistema con una cuenta con derechos de administrador.
2. Cambie de directorio a la carpeta de instalación de Kaspersky Security Center (generalmente, C:\Archivos de programa (x86)\Kaspersky Lab\Kaspersky Security Center).
3. Ingrese el siguiente comando (recuerde utilizar derechos de administrador):
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<direcciones IP>" -t s`

   Introduzca las direcciones IP que haya recopilado siguiendo los criterios de más arriba. Utilice un punto y coma para separar cada dirección.

   Ejemplo para permitir que un solo dispositivo se conecte al Servidor de administración:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s`

   Ejemplo para permitir que varios dispositivos se conecten al Servidor de administración:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s`
4. Reinicie el servicio del Servidor de administración.

Para saber si la lista de direcciones IP permitidas se definió correctamente, consulte el registro de eventos de Kaspersky en el Servidor de administración.

## Cómo modificar una lista de direcciones IP permitidas

Para modificar una lista de direcciones permitidas, puede seguir los mismos pasos que utilizó para crearla. Ejecute el mismo comando que la primera vez y defina una nueva lista:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<direcciones IP>" -t s
```

Si desea eliminar algunas direcciones IP de la lista de admitidos, debe reescribirla. Por ejemplo, su lista de admitidos incluye las siguientes direcciones IP: 192.0.2.0; 198.51.100.0; 203.0.113.0. Desea eliminar la dirección IP 198.51.100.0. Para hacer esto, ingrese el siguiente comando en el símbolo del sistema:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0;
203.0.113.0" -t s
```

No olvide reiniciar el servicio del Servidor de administración.

### Cómo eliminar una lista de direcciones IP permitidas

*Si ya ha definido una lista de direcciones IP permitidas y desea eliminarla:*

1. Ingrese el siguiente comando en el símbolo del sistema (recuerde utilizar derechos de administrador):
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`

2. Reinicie el servicio del Servidor de administración.

Una vez que complete estos pasos, el control de direcciones IP quedará deshabilitado.

## Usar la utilidad klscflag para cerrar el puerto 13291

El Servidor de administración utiliza el puerto 13291 para recibir conexiones de las consolas de administración. La aplicación abre este puerto de manera predeterminada. Si no desea utilizar la Consola de administración basada en MMC o la utilidad klakaut, puede cerrar el puerto a través de la utilidad klscflag. La utilidad cambia el valor del parámetro KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

*Para cerrar el puerto 13291:*

1. Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada es <Disk>:\Archivos de programa(x86)\Kaspersky Lab\Kaspersky Security Center.

2. Ejecute el siguiente comando en la línea de comandos:
   ```
   klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv false -
   svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
   ```

3. Reinicie el servicio del Servidor de administración de Kaspersky Security Center.

   El puerto 13291 queda cerrado.

*Para verificar que el puerto 13291 se haya cerrado:*

Ejecute el siguiente comando en la línea de comandos:

```
klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -
ss "|ss_type = \"SS_SETTINGS\";"
```

El comando dará el siguiente resultado:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)false
```

El valor `false` indica que el puerto está cerrado. Si el puerto estuviera abierto, se mostraría el valor `true`.

## Desconexión de un Servidor de administración

*Para desconectarse de un Servidor de administración:*

1. En el árbol de consola, seleccione el nodo correspondiente al Servidor de administración que desea desconectar.
2. En el menú contextual del nodo, seleccione **Desconectarse del Servidor de administración**.

## Agregar un Servidor de administración al árbol de consola

*Para agregar un nuevo Servidor de administración al árbol de consola:*

1. En la ventana principal de Kaspersky Security Center, en el árbol de la consola, seleccione el nodo de **Kaspersky Security Center**.
2. En el menú contextual del nodo, seleccione **Nuevo → Servidor de administración**.

Se creará un nodo denominado **Servidor de administración - <Nombre del dispositivo> (no conectado)** en el árbol de consola, desde el cual se podrá conectar a cualquier Servidor de administración instalado en la red.

## Eliminación de un Servidor de administración del árbol de consola

*Eliminar un Servidor de administración del árbol de consola:*

1. En el árbol de consola, seleccione el nodo correspondiente al Servidor de administración que desea eliminar.
2. En el menú contextual del nodo, seleccione **Eliminar**.

## Agregar un Servidor de administración virtual al árbol de consola

*Para agregar un nuevo Servidor de administración virtual al árbol de consola:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración para el que necesita crear un Servidor de administración virtual.
2. En el nodo Servidor de administración, seleccione la carpeta **Servidores de administración**.
3. En el espacio de trabajo de la carpeta **Servidores de administración**, haga clic en el enlace **Agregar un Servidor de administración virtual**.

   Se inicia el Asistente para crear un Servidor de administración virtual.
4. En la ventana **Nombre del Servidor de administración virtual**, especifique el nombre del Servidor de administración virtual que se creará.

   El nombre del Servidor de administración virtual no puede contener más de 255 caracteres de largo y no puede incluir ningún carácter especial (como "*<>-_?:\|).

5. En la ventana **Escriba la dirección que los dispositivos usarán para conectarse al Servidor de administración virtual**, especifique la dirección de conexión del dispositivo

   La dirección de conexión de un Servidor de administración virtual es la dirección de red mediante la cual los dispositivos se conectarán a ese Servidor. La dirección de conexión tiene dos partes: la dirección de red de un Servidor de administración físico y, separado con una barra, el nombre de un Servidor de administración virtual. El nombre del Servidor de administración virtual se sustituirá automáticamente. La dirección especificada se utilizará en el Servidor de administración virtual como dirección predeterminada en los paquetes de instalación del Agente de red.

6. En la ventana **Crear la cuenta del administrador del Servidor de administración virtual**, designe a un usuario de la lista para que funcione como el administrador del Servidor virtual o agregue una nueva cuenta de administrador haciendo clic en el botón **Crear**.

   Puede especificar varias cuentas.

Se crea un nodo denominado **Servidor de administración <nombre del Servidor de administración virtual>** en el árbol de la consola.

## Cambio de una cuenta de servicio del Servidor de administración Utilidad klsrvswch

Si necesita cambiar la cuenta de servicio del Servidor de administración configurada al instalar Kaspersky Security Center, puede usar una utilidad denominada klsrvswch, diseñada para cambiar la cuenta del Servidor de administración.

Al instalar Kaspersky Security Center, la utilidad se copia automáticamente en la carpeta de instalación de la aplicación.

El número de inicios de la utilidad es esencialmente ilimitado.

Debe iniciar la utilidad klsrvswch en el dispositivo del Servidor de administración en la cuenta con derechos de administrador que se utilizó para instalar el Servidor de administración.

La utilidad klsrvswch permite cambiar el tipo de cuenta. Por ejemplo, si utiliza una cuenta local, puede cambiarla a una cuenta de dominio o a una cuenta de servicio administrada (y viceversa). La utilidad klsrvswch no le permite cambiar el tipo de cuenta a cuenta de servicio administrado por grupo (gMSA).

Windows Vista y las versiones posteriores de Windows no permiten el uso de una cuenta del sistema local para el Servidor de administración. En estas versiones de Windows, la opción **Cuenta del sistema local** está inactiva.

*Para cambiar una cuenta de servicio del Servidor de administración a una cuenta de dominio:*

1. Inicie la utilidad klsrvswch desde la carpeta de instalación de Kaspersky Security Center. La ruta de instalación predeterminada: <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Esta acción inicia también el asistente para la modificación de la cuenta de servicio del Servidor de administración. Siga las instrucciones del asistente.

2. En la ventana **Cuenta de servicio del Servidor de administración**, seleccione **Cuenta del sistema local**.

Una vez que finalice el asistente, se modificará la cuenta del Servidor de administración. El servicio del Servidor de administración se iniciará mediante la *Cuenta del sistema local*, utilizando sus credenciales.

El funcionamiento correcto de Kaspersky Security Center requiere que la cuenta utilizada para iniciar el servicio del Servidor de administración posea los derechos de administrador del recurso donde se aloja la base de datos del Servidor de administración.

*Para cambiar una cuenta de servicio del Servidor de administración a una cuenta de usuario o a una cuenta de servicio administrada:*

1. Inicie la utilidad klsrvswch desde la carpeta de instalación de Kaspersky Security Center. La ruta de instalación predeterminada: <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Esta acción inicia también el asistente para la modificación de la cuenta de servicio del Servidor de administración. Siga las instrucciones del asistente.

2. En la ventana **Cuenta de servicio del Servidor de administración**, seleccione **Cuenta personalizada**.

3. Haga clic en el botón **Buscar ahora**.

   Se abre la ventana **Seleccionar el usuario**.

4. En la ventana **Seleccionar el usuario**, haga clic en el botón **Tipos de objetos**.

5. En la lista de tipos de objeto, seleccione **Usuarios** (si desea una cuenta de usuario) o **Cuentas de servicio** (si desea una cuenta de servicio administrada) y haga clic en **Aceptar**.

6. En el campo Nombre del objeto, introduzca el nombre de la cuenta o una parte del nombre y haga clic en **Comprobar nombres**.

7. En la lista de nombres coincidentes, seleccione el nombre necesario y, a continuación, haga clic en **Aceptar**.

8. Si seleccionó **Cuentas de servicio**, en la ventana **Contraseña de la cuenta**, deje en blanco los campos **Contraseña** y **Confirmar contraseña**. Si ha seleccionado **Usuarios**, introduzca una nueva clave de acceso para el usuario y confírmela.

La cuenta de servicio del Servidor de administración se cambiará a la cuenta que haya seleccionado.

Al usar Microsoft SQL Server en un modo que presupone la autenticación de cuentas de usuario con herramientas de Windows, debe otorgarse el acceso a la base de datos. La cuenta de usuario debe contar con el estado del propietario de la base de datos de Kaspersky Security Center. El esquema propietario de base de datos (dbo) se utiliza de manera predeterminada.

## Cambio de las credenciales de DBMS

En algunas ocasiones es posible que deba cambiar las credenciales de DBMS, por ejemplo, para realizar una rotación de credenciales por motivos de seguridad.

*Para cambiar las credenciales de DBMS en un entorno de Windows mediante klsrvswch.exe, siga estos pasos:*

1. Inicie la utilidad klsrvswch ubicada en la carpeta de instalación de Kaspersky Security Center. La ruta de instalación predeterminada: <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Debe iniciar la utilidad klsrvswch en el dispositivo del Servidor de administración en la cuenta con derechos de administrador que se utilizó para instalar el Servidor de administración.

2. Haga clic en el botón **Siguiente** del Asistente hasta llegar al paso **Cambiar las credenciales de acceso al DBMS**.

3. En el paso **Cambiar las credenciales de acceso al DBMS** del asistente, haga lo siguiente:

   El paso **Cambiar las credenciales de acceso al DBMS** del asistente se omite si se utiliza la autenticación de Windows.

   - Seleccione la opción **Aplicar credenciales nuevas**.
   - Especifique un nuevo nombre de cuenta en el campo **Cuenta**.
   - Especifique una nueva contraseña para una cuenta en el campo **Contraseña**.
   - Especifique la nueva contraseña en el campo **Confirmar contraseña**.

   Debe especificar las credenciales de una cuenta que exista en el DBMS.

4. Haga clic en el botón **Siguiente**.

Una vez finalizado el asistente, se cambian las credenciales de DBMS.

La utilidad klsrvswch solo se puede utilizar para cambiar la contraseña de la cuenta para la autenticación de SQL. No se admite cambiar el método de autorización. Para cambiar el método de autorización, reinstale el Servidor de administración y especifique la configuración deseada.

## Cambiar la carpeta compartida del Servidor de administración

La carpeta compartida del Servidor de administración se especifica durante la instalación del Servidor de administración. Puede cambiar la ubicación de la carpeta compartida en las propiedades del Servidor de administración.

*Para cambiar la carpeta compartida:*

1. Cree una carpeta compartida de red y configure los permisos para el recurso compartido y para la estructura de carpetas a fin de permitir los derechos de control total para el subgrupo **Todos**.

2. En el árbol de la consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y seleccione **Propiedades**.

3. En la ventana de propiedades del Servidor de administración, en el panel **Secciones**, seleccione **Avanzado** y luego seleccione **Carpeta compartida del Servidor de administración**.

4. En la sección **Carpeta compartida del Servidor de administración**, haga clic en el botón **Cambiar**.
5. Seleccione la carpeta que desea usar como compartida.
6. Haga clic en el botón **Aceptar** para cerrar la ventana de propiedades del Servidor de administración.
7. Asignar derechos de lectura para el subgrupo **Todos** para la carpeta que seleccionó como compartida.

# Resolución de problemas con los nodos del Servidor de administración

El árbol de la consola en el panel izquierdo de la Consola de administración contiene nodos de Servidores de administración. Puede añadir al árbol de la consola todos los Servidores de administración que necesite.

La lista de nodos del Servidor de administración en el árbol de la consola se almacena en una copia paralela de un archivo .msc por medio de la Consola de administración de Microsoft. La copia paralela de este archivo se encuentra en la carpeta %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ del dispositivo en que está instalada la Consola de administración. Para cada nodo del Servidor de administración, el archivo contiene esta información:

- Dirección del Servidor de administración
- Número de puerto
- Si TLS está en uso

  Este parámetro depende del número de puerto utilizado para conectar la Consola de administración al Servidor de administración.
- Nombre de usuario
- Certificado del Servidor de administración

## Resolución de problemas

Cuando la Consola de administración se conecta al Servidor de administración, el certificado almacenado localmente se compara con el Certificado del Servidor de administración. Si los certificados no coinciden, la Consola de administración genera un error. Por ejemplo, podría haber una discrepancia de certificados al reemplazar el Certificado del Servidor de administración. En ese caso, vuelva a crear el nodo del Servidor de administración en la consola.

*Para volver a crear un nodo de Servidor de administración:*

1. Cierre la ventana de la Consola de administración de Kaspersky Security Center.
2. Elimine el archivo de Kaspersky Security Center 15.1 en %USERPROFILE%\AppData\Roaming\Microsoft\MMC\.

3. Ejecute la Consola de administración de Kaspersky Security Center.

   Se le pedirá que se conecte al Servidor de administración y acepte el certificado existente.

4. Realice una de las siguientes acciones:

   - Acepte el certificado existente haciendo clic en el botón **Sí**.
   - Para especificar su certificado, haga clic en el botón **No** y luego vaya al archivo del certificado que usar para autenticar el Servidor de administración.

El problema de certificado queda resuelto. Puede utilizar la Consola de administración para conectar con el Servidor de administración.

# Visualización y modificación de la configuración de un Servidor de administración

Puede ajustar la configuración de un Servidor de administración en la ventana de propiedades de este Servidor.

*Para abrir la ventana "Propiedades: Servidor de administración",*

Seleccione **Propiedades** en el menú contextual del nodo del Servidor de administración en el árbol de consola.

## Ajuste de la configuración general del Servidor de administración

Se puede ajustar la configuración general de un Servidor de administración en las secciones **General**, **Configuración de conexión del Servidor de administración**, **Repositorio de eventos** y **Seguridad** de la ventana Propiedades del Servidor de administración.

La sección **Seguridad** no se muestra en la ventana de propiedades del Servidor de administración si se deshabilitó su visualización en la interfaz de la Consola de administración.

*Para habilitar la visualización de la sección **Seguridad** en la Consola de administración:*

1. En el árbol de la consola, seleccione el Servidor de administración que desee.
2. En el menú **Ver** de la ventana principal de la aplicación, seleccione **Configuración de interfaz**.
3. En la ventana **Configuración de interfaz** que se abre, seleccione la casilla de verificación **Mostrar secciones de configuración de seguridad** y haga clic **Aceptar**.
4. En la ventana con el mensaje de la aplicación, haga clic en **Aceptar**.

Ahora se mostrará la sección **Seguridad** en la ventana de propiedades del Servidor de administración.

## Configuración de la interfaz de la Consola de administración

Puede ajustar la configuración de la interfaz de la Consola de administración para mostrar u ocultar los controles de la interfaz de usuario relacionados con las siguientes funciones:

- Administración de vulnerabilidades y parches
- Protección y cifrado de datos
- Configuración de Control de Endpoint
- Administración de dispositivos móviles
- Servidores de administración secundarios
- Secciones de configuración de seguridad

*Para ajustar la configuración de la interfaz de la Consola de administración, realice lo siguiente:*

1. En el árbol de la consola, seleccione el Servidor de administración que desee.
2. En el menú **Ver** de la ventana principal de la aplicación, seleccione **Configuración de interfaz**.
3. En la ventana **Configuración de interfaz** que se abre, seleccione las casillas junto a las funciones que desea mostrar y haga clic en **Aceptar**.
4. En la ventana con el mensaje de la aplicación, haga clic en **Aceptar**.

Las funciones seleccionadas se mostrarán en la interfaz de la Consola de administración.

## Almacenamiento y procesamiento de eventos en el Servidor de administración

La información sobre eventos que ocurren durante la operación de la aplicación y los dispositivos administrados se guarda en la base de datos del Servidor de administración. A cada evento se le atribuye un tipo y un nivel de gravedad (*Evento crítico*, *Error funcional*, *Advertencia* o *Información*). Según las condiciones en las que se produce un evento, la aplicación puede asignar diferentes niveles de gravedad a eventos del mismo tipo.

Se pueden ver los tipos y niveles de gravedad asignados a los eventos en la sección **Configuración de eventos** de la ventana de propiedades del Servidor de administración. En la sección **Configuración de eventos**, también puede configurar el procesamiento de todos los eventos por parte del Servidor de administración:

- El registro de eventos en el Servidor de administración y en los registros de eventos del sistema operativo en un dispositivo y en el Servidor de administración.
- El método utilizado para notificar al administrador acerca de un evento (por ejemplo, un mensaje de texto o un mensaje de correo electrónico).

En la sección **Repositorio de eventos** de la ventana de propiedades del Servidor de administración, puede editar la configuración del almacenamiento de eventos en la base de datos del Servidor de administración limitando el número de registros de eventos o el tiempo de almacenamiento de los registros. Cuando se especifica el número máximo de eventos, la aplicación calcula una cantidad aproximada de espacio de almacenamiento requerido para el número especificado. Puede utilizar este cálculo aproximado para evaluar si tiene suficiente espacio libre en el disco para evitar el desbordamiento de la base de datos. La capacidad predeterminada de la base de datos del Servidor de administración es de 400 000 eventos. La capacidad máxima recomendada de la base de datos es de 45 millones de eventos.

La aplicación comprueba la base de datos cada 10 minutos. Si la cantidad de eventos alcanza el valor máximo especificado más 10 000, la aplicación elimina los eventos más antiguos para que solo quede la cantidad máxima de eventos especificada.

Cuando el Servidor de administración elimina los eventos antiguos, no puede guardar los nuevos eventos en la base de datos. Durante este período de tiempo, la información sobre los eventos que fueron rechazados se escribe en el Registro de eventos de Kaspersky. Los nuevos eventos se ponen en cola y se guardan en la base de datos una vez finalizada la operación de borrado.

Puede cambiar la configuración de cualquier tarea para guardar eventos relacionados con el progreso de la misma, o guardar solo los resultados de la ejecución de la tarea. Al hacerlo, reducirá la cantidad de eventos en la base de datos, aumentará la velocidad de ejecución de los escenarios asociados con el análisis de la tabla de eventos en la base de datos y disminuirá el riesgo de que una gran cantidad de eventos sobrescriban eventos críticos.

## Visualización del registro de conexiones al Servidor de administración

El historial de conexiones e intentos de conexión con el Servidor de administración durante su funcionamiento se puede guardar en un archivo de registro. La información en el archivo le permite rastrear no solo las conexiones de su infraestructura de red, sino también los intentos no autorizados de acceder al Servidor de administración.

*Para registrar los eventos de conexión al Servidor de administración:*

1. En el árbol de la consola, seleccione el Servidor de administración para el que necesita activar el registro de eventos de conexión.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
3. En la ventana de propiedades que se abre, en la sección **Configuración de conexión del Servidor de administración**, seleccione la subsección **Puertos de conexión**.
4. Habilitar la opción **Registrar historial de conexiones recibidas por el Servidor de administración**.
5. Haga clic en el botón **Aceptar** para cerrar la ventana de propiedades del Servidor de administración.

Todos los eventos adicionales de la conexión con el Servidor de administración, los resultados de autenticación y los errores de SSL se guardarán en el archivo %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog.

## Control de brotes de virus

Kaspersky Security Center le permite responder rápidamente a las amenazas emergentes de brotes de virus. Los riesgos de los brotes de virus se evalúan mediante la supervisión de la actividad de virus en dispositivos cliente.

Puede configurar reglas de evaluación para amenazas de brotes de virus y las medidas que se deben tomar en caso de que surja alguno. Para hacer esto, use la sección **Brote de virus** de la ventana de propiedades del Servidor de administración.

Puede especificar el procedimiento de notificación para el evento *Brote de virus* en la sección **Configuración de eventos** de la ventana de propiedades del Servidor de administración, en la ventana de propiedades del evento *Brote de virus*.

El evento *Brote de virus* se genera si se detectan eventos *Objeto malicioso detectado* durante la utilización de aplicaciones de seguridad. Por lo tanto, debe guardar la información de todos los eventos *Objeto malicioso detectado* en el Servidor de administración para reconocer los brotes de virus.

Puede especificar la configuración para guardar la información acerca de los eventos *Objeto malicioso detectado* en las directivas de las aplicaciones de seguridad.

Al contar los eventos *Objeto malicioso detectado*, solamente se tomará en cuenta la información de los dispositivos del Servidor de administración principal. La información de los Servidores de administración secundarios no se toma en cuenta. La configuración del evento *Brote de virus* se ajusta individualmente para cada Servidor secundario.

## Límite de tráfico

Para reducir los volúmenes de tráfico dentro de una red, la aplicación proporciona la opción de limitar la velocidad de transferencia de datos a un Servidor de administración desde los intervalos IP y subredes IP especificados.

Se pueden crear y configurar reglas de límite de tráfico en la sección **Tráfico** de la ventana de propiedades del Servidor de administración.

*Para crear una regla de límite de tráfico:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración para el que desee crear una regla de límite de tráfico.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
3. En la ventana de propiedades del Servidor de administración, seleccione la sección **Tráfico**.

4. Haga clic en el botón **Agregar**.

5. En la ventana **Nueva regla**, especifique los siguientes ajustes:

   En la sección **Intervalo IP para limitar el tráfico**, seleccione el método que se utilizará para definir la subred o el intervalo que limitará la transferencia de datos y, a continuación, ingrese los valores de los parámetros correspondientes al método seleccionado. Seleccione uno de los siguientes métodos:

   - **Especifique el intervalo usando una dirección y máscara de red**

     El tráfico se limita según la configuración de la subred. Especifique la dirección de subred y la máscara de subred para determinar el intervalo en el cual el tráfico se limitará.

     También puede hacer clic en **Examinar** para agregar subredes de la lista global de subredes.

   - **Especifique el intervalo usando las direcciones inicial y final**

     El tráfico se limita según un rango de Direcciones IP. Especifique el rango de direcciones IP en los campos de entrada **Inicio** y **Fin**.

     Esta opción está seleccionada de forma predeterminada.

   En la sección **Límite de tráfico**, puede ajustar la configuración restrictiva siguiente del índice de transferencia de datos:

   - **Intervalo de tiempo**

     Intervalo de tiempo durante el que estará vigente la restricción de tráfico. Puede especificar los límites del intervalo de tiempo en los campos de entrada.

   - **Límite (KB/s)**

     Velocidad de transferencia total máxima de datos de entrada y datos de salida del Servidor de administración. La restricción de tráfico solo será efectiva en un intervalo especificado en el campo **Intervalo de tiempo**.

   - **Limitar tráfico para el resto del tiempo (KB/s)**

     El tráfico no se limitará únicamente durante el intervalo especificado en el campo **Intervalo de tiempo**, sino también en otros momentos.

     Esta casilla no está marcada de manera predeterminada. El valor de este campo puede no coincidir con el valor del campo **Límite (KB/s)**.

Principalmente, las reglas de limitación de tráfico afectan la transferencia de archivos. Estas reglas no se aplican al tráfico generado por la sincronización entre el Servidor de administración y el Agente de red, o entre Servidores de administración principales y secundarios.

## Configuración del Servidor web

El Servidor Web está diseñado para publicar paquetes de instalación independientes, perfiles de MDM para iOS y archivos de la carpeta compartida.

Puede definir la configuración de la conexión del Servidor web al Servidor de administración y configurar un certificado de Servidor web en la sección **Servidor web** de la ventana de propiedades del Servidor de administración.

### Trabajar con usuarios internos

Las cuentas de *usuarios internos* se utilizan para trabajar con Servidores de administración virtuales. Kaspersky Security Center otorga los permisos de usuarios reales a los usuarios internos de la aplicación.

Las cuentas de los usuarios internos se crean y utilizan solo para trabajar dentro de Kaspersky Security Center. No se transfiere ningún dato sobre estos usuarios internos al sistema operativo. Kaspersky Security Center se encarga de autenticar a los usuarios internos.

Puede configurar cuentas de usuarios internos en la carpeta **Cuentas de usuario** del árbol de la consola.

## Copia de seguridad y restauración de la configuración del Servidor de administración

La copia de seguridad de la configuración del Servidor de administración y su base de datos se realiza a través de la tarea de copia de seguridad y la utilidad klbackup. Una copia de seguridad incluye toda la configuración principal y objetos que pertenecen al Servidor de administración, por ejemplo, certificados, claves maestras para el cifrado de unidades en dispositivos administrados, claves para varias licencias, estructura de grupos de administración con todos sus contenidos, tareas, directivas, etc. Con una copia de seguridad puede recuperar la operación de un Servidor de administración cuanto antes, lo que puede demorar de una docena de minutos a un par de horas.

Si ninguna copia de seguridad está disponible, un error puede llevar a una pérdida irrevocable de certificados y toda la configuración del Servidor de administración. Esto requerirá a configurar de nuevo Kaspersky Security Center desde el principio y realizar la distribución inicial del Agente de red en la red de la organización de nuevo. Todas las claves principales para el cifrado de unidades en dispositivos administrados también se perderán, arriesgando la pérdida irrevocable de datos cifrados en dispositivos con Kaspersky Endpoint Security. Por ese motivo, no debe descuidar las copias de seguridad habituales del Servidor de administración usando la tarea de copia de seguridad estándar.

El Asistente de inicio rápido crea la tarea de copia de seguridad para la configuración del Servidor de administración y lo configura para que se ejecute a diario, a las 4:00 a. m. Las copias de seguridad se guardan de forma predeterminada en la carpeta %ALLUSERSPROFILE%\Application Data\KasperskySC.

Si una instancia de Microsoft SQL Server instalada en otro dispositivo se utiliza como DBMS, debe modificar la tarea de copia de seguridad al especificar una ruta de UNC, que está disponible para escritura tanto de parte del servicio del Servidor de administración como del servicio de SQL Server, como la carpeta para almacenar copias de seguridad. Este requisito se deriva de una característica especial de copia de seguridad en DBMS de Microsoft SQL Server.

Si una instancia local de Microsoft SQL Server se utiliza como DBMS, también recomendamos guardar copias de seguridad en un medio dedicado a fin de asegurarlos contra el daño junto con el Servidor de administración.

Como una copia de seguridad contiene datos importantes, la tarea de copia de seguridad y la utilidad klbackup aseguran la protección con contraseña de copias de seguridad. De forma predeterminada, la tarea de copia de seguridad se crea con una contraseña en blanco. Debe configurar una contraseña en las propiedades de la tarea de copia de seguridad. Descuidar este requisito causa una situación donde todas las claves de certificados del Servidor de administración, las claves para licencias y las claves principales para el cifrado de unidades en dispositivos administrados permanecen no cifradas.

Además de la copia de seguridad habitual, también debe crear una copia de seguridad antes de cada cambio significativo, incluida la instalación de actualizaciones del Servidor de administración y los parches.

Si utiliza Microsoft SQL Server como DBMS, puede minimizar el tamaño de las copias de seguridad. Para ello, habilite la opción **Comprimir copia de seguridad** en la configuración de SQL Server.

Para restaurar una copia de seguridad, deberá utilizar la utilidad klbackup en una instancia del Servidor de administración que se acabe de instalar, que esté en funcionamiento y que sea de la misma versión para la que se haya creado la copia de seguridad (o de una versión más reciente).

La instancia del Servidor de administración en el cual se debe realizar la restauración debe utilizar un DBMS del mismo tipo (por ejemplo, el mismo SQL Server o MariaDB) y la misma versión o una posterior. La versión del Servidor de administración puede ser igual (con un parche idéntico o posterior) o posterior.

Esta sección describe situaciones estándares para restaurar la configuración y objetos del Servidor de administración.

## Uso de una instantánea del sistema de archivos para reducir la duración de la copia de seguridad

En Kaspersky Security Center 15.1, el tiempo de inactividad del Servidor de administración durante la copia de seguridad se ha reducido en comparación con las versiones anteriores. Además, se ha agregad la función **Usar instantánea de sistema de archivos para copia de seguridad de datos** a las configuraciones de la tarea. Esta característica proporciona una reducción de inactividad adicional mediante el uso de la utilidad klbackup, que crea una "instantánea" del disco durante la copia de seguridad (esto toma unos segundos) y simultáneamente copia la base de datos (esto solo demora unos minutos como máximo). Cuando klbackup crea una instantánea del disco y una copia de la base de datos, la herramienta permite que el Servidor de administración se pueda volver a conectar.

Puede utilizar la función de captura de instantáneas del sistema de archivos solo si se cumplen estas dos condiciones:

- La carpeta compartida del Servidor de administración y la carpeta %ALLUSERSPROFILE%\KasperskyLab están ubicadas en el mismo disco lógico y son locales en referencia al Servidor de administración.
- La carpeta %ALLUSERSPROFILE%\KasperskyLab no contiene ningún enlace simbólico que se haya creado manualmente.

No use la función si cualquiera de estas condiciones no se cumple. En este caso, la aplicación devolverá un mensaje de error en respuesta a cualquier intento de crear una instantánea del sistema de archivos.

Para usar la función, debe tener una cuenta a la que se le haya otorgado el permiso para crear instantáneas del disco lógico que almacena la carpeta %ALLUSERSPROFILE%. Tenga en cuenta que la cuenta de servicio del Servidor de administración no tiene tal permiso.

*Para usar la función de captura de instantáneas del sistema de archivos para reducir la duración de la copia de seguridad:*

1. En la sección **Tareas**, seleccione la tarea de copia de seguridad.
2. En el menú contextual, seleccione **Propiedades**.
3. En la ventana de las propiedades de la tarea que se abre, seleccione la sección **Configuración**.

4. Seleccione la casilla **Usar instantánea del sistema de archivos para la copia de seguridad de datos**.

5. En los campos **Nombre de usuario** y **Contraseña**, ingrese el nombre y la contraseña de una cuenta que tenga permiso para crear instantáneas del disco lógico que almacena la carpeta % ALLUSERSPROFILE%.

6. Haga clic en **Aplicar**.

En cualquier inicio posterior de la tarea de copia de seguridad, la utilidad klbackup creará instantáneas del sistema de archivos reduciendo así el tiempo de inactividad del Servidor de administración durante la ejecución de la tarea.

## Un dispositivo con el Servidor de administración es inoperable

Si un dispositivo con el Servidor de administración es inoperable debido a un error, se recomiendan realizar las siguientes acciones:

- Se debe asignar al nuevo Servidor de administración la misma dirección: nombre NetBIOS, FQDN o IP estática (dependiendo de cuál se haya definido al instalarse los Agentes de red).

- Instalar el Servidor de administración usando un DBMS del mismo tipo, de la misma versión (o una posterior). Puede instalar la misma versión del Servidor con el mismo parche (o uno posterior), o una versión posterior. Después de la instalación, no realice la instalación inicial a través del Asistente.

- En el menú **Iniciar**, ejecute la utilidad klbackup y realice la restauración.

## La configuración del Servidor de administración o la base de datos es corrupta

Si el Servidor de administración es inoperable debido a configuración o la base de datos corruptas (por ejemplo, después de una sobrecarga eléctrica), se recomienda usar la siguiente situación de restauración:

1. Analice el sistema de archivos en el dispositivo dañado.

2. Desinstale la versión inoperable del Servidor de administración.

3. Reinstale el Servidor de administración usando un DBMS del mismo tipo y de la misma versión (o una posterior). Puede instalar la misma versión del Servidor con el mismo parche (o uno posterior), o una versión posterior. Después de la instalación, no realice la instalación inicial a través del Asistente.

4. En el menú **Iniciar**, ejecute la utilidad klbackup y realice la restauración.

Se prohíbe restaurar el Servidor de administración de cualquier modo diferente de a través de la utilidad klbackup.

Cualquier intento de restaurar el Servidor de administración a través de un software de terceros llevará inevitablemente a la desincronización de datos en los nodos de Kaspersky Security Center de la aplicación distribuida y, por consiguiente, al funcionamiento inadecuado de la aplicación.

# Copia de seguridad y restauración de los datos del Servidor de administración

La copia de seguridad de datos le permite mover un Servidor de administración de un dispositivo a otro, sin pérdida de datos. Mediante la copia de seguridad, puede restaurar datos al mover las bases de datos del Servidor de Administración a otro dispositivo o al actualizar a una versión más nueva de Kaspersky Security Center. Además, puede usar la copia de seguridad de datos para mover datos del Servidor de Administración desde Kaspersky Security Center Windows y ponerlos bajo la administración de Kaspersky Security Center Linux (no se admite mover datos de Kaspersky Security Center Linux a Kaspersky Security Center Windows).

No se realiza una copia de seguridad de los complementos de administración instalados. Después de restaurar los datos del Servidor de administración a partir de una copia de seguridad, debe descargar y volver a instalar los complementos para las aplicaciones administradas.

Antes de crear una copia de seguridad de los datos del Servidor de administración, verifique si se agregó un Servidor de administración virtual al grupo de administración. Si se agrega un Servidor de administración virtual, asegúrese de que se asigne un administrador a este Servidor de administración virtual antes de realizar la copia de seguridad. No puede otorgar derechos de acceso de administrador al Servidor de administración virtual después de la copia de seguridad. Tenga en cuenta que si se pierden las credenciales de la cuenta de administrador, no podrá asignar un nuevo administrador al Servidor de administrador virtual.

Para hacer un respaldo o restaurar un clúster de conmutación por error de Kaspersky Security Center, debe detener todo el clúster para realizar el mantenimiento y, luego, reiniciarlo cuando se complete el respaldo o la restauración.

Puede crear una copia de seguridad de los datos del Servidor de administración mediante uno de los siguientes métodos:

- Al crear y ejecutar una tarea de copia de seguridad de datos utilizando la Consola de administración.
- Puede ejecutar la utilidad klbackup en el dispositivo que tiene instalado el Servidor de administración. Esta utilidad está incluida en el kit de distribución de Kaspersky Security Center. Una vez instalado el Servidor de administración, la encontrará en la raíz de la carpeta de destino especificada durante la instalación de la aplicación.

Se guardan los siguientes datos en la copia de seguridad del Servidor de administración:

- Base de datos del Servidor de administración (directivas, tareas, parámetros de la aplicación, eventos guardados en el Servidor de administración).
- Información de configuración de la estructura de los grupos de administración y los dispositivos cliente.
- Repositorio de paquetes de distribución de aplicaciones para instalación remota.
- Certificado del Servidor de administración.
- Contenido de la carpeta *Actualizaciones*.

  De forma predeterminada, la ruta de la carpeta es C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\

La restauración de los datos del Servidor de administración solo se puede realizar mediante la utilidad klbackup. Para llevar a cabo la restauración en una instancia del Servidor de administración que se acaba de instalar, que esté en funcionamiento y que sea de la misma versión para la que se haya creado la copia de seguridad (o de una versión más reciente).

## Tarea Copia de seguridad de los datos del Servidor de administración

### Crear una tarea Copia de seguridad de los datos del Servidor de administración

La tarea Copia de seguridad es una tarea del Servidor de administración que se crea a través del asistente de inicio rápido. Si se elimina una tarea de copia de seguridad creada por el asistente de inicio rápido, puede crearse otra manualmente.

*Para crear una tarea Copia de seguridad de los datos del Servidor de administración:*

1. En el árbol de la consola, seleccione la carpeta **Tareas**.
2. Realice una de las siguientes acciones para comenzar a crear la tarea:
   - Seleccione **Nuevo → Tarea** en el menú contextual de la carpeta **Tareas** en el árbol de la consola.
   - Haga clic en el botón **Crear una tarea** en el espacio de trabajo.

   Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente. En la ventana **Seleccione el tipo de tarea** del asistente, seleccione el tipo de tarea denominado **Copia de seguridad de los datos del Servidor de administración**.

La tarea **Copia de seguridad de los datos del Servidor de administración** solo puede crearse en una sola copia. Si la tarea de copia de seguridad de los datos del Servidor de administración ya fue creada para el Servidor de administración, no se mostrará en la ventana de selección del tipo de tarea del Asistente de creación de tareas de copia de seguridad.

## Configurar la tarea Copia de seguridad de los datos del Servidor de administración

Después de crear una tarea de copia de seguridad, puede configurar sus ajustes.

*Para configurar la tarea Copia de seguridad de los datos del Servidor de administración:*

1. En el árbol de la consola, seleccione la carpeta **Tareas**.
2. En el menú contextual de la tarea **Copia de seguridad de los datos del Servidor de administración**, seleccione **Propiedades**.

Se abre la ventana de propiedades de la tarea *Copia de seguridad de los datos del Servidor de administración*. Están disponibles las siguientes propiedades:

- **General**

  En la sección **General**, puede especificar el nombre de la tarea, ver la fecha de creación de la tarea, la fecha del último comando, los estados de las ejecuciones de la tarea y los resultados de la tarea.

- **Notificación**

  En la sección **Notificación**, puede especificar la configuración para eventos relacionados con los resultados de la ejecución de la tarea, así como configurar las notificaciones sobre los resultados de la ejecución de la tarea.

- **Programación**

  En la sección **Programación**, puede especificar una programación para el inicio de la tarea.

- **Destino**

  En la sección **Destino**, puede especificar la ruta a la carpeta que almacenará las copias de seguridad de los datos del Servidor de administración.

- **Configuración**

  En la sección **Configuración**, puede establecer la contraseña de protección de la copia de seguridad y la cantidad de copias de seguridad si es necesario.

  También puede crear una copia paralela del disco lógico que almacena la carpeta %ALLUSERSPROFILE% y copiar la base de datos del Servidor de administración. Para hacer esto, debe habilitar la opción **Usar una instantánea del sistema de archivos para crear las copias de seguridad** y, luego, especificar el nombre y la contraseña de una cuenta que tenga permiso para crear instantáneas.

- **Seguridad**

  En la sección **Seguridad**, puede otorgar permisos a usuarios y grupos para realizar operaciones en el Servidor de administración. Si la opción **Heredar configuración del Servidor de administración** está habilitada, la configuración de seguridad de la tarea se hereda del Servidor de administración.

  Si esta opción está deshabilitada, puede configurar los ajustes de seguridad para la tarea. Puede asignar una función a un usuario o un grupo de usuarios o asignar permisos a un usuario o un grupo de usuarios, según se aplique a la tarea.

  De manera predeterminada, la opción **Heredar configuración del Servidor de administración** está habilitada.

- **Historial de revisiones**

  En la sección **Historial de revisiones**, puede hacer un seguimiento de la modificación de la tarea. Cuando una tarea se modifica de algún modo, se crea una revisión.

## Utilidad de copia de seguridad y recuperación de datos (klbackup)

Puede copiar datos del Servidor de administración para crear copias de seguridad y futura recuperación mediante la utilidad klbackup que forma parte del kit de distribución de Kaspersky Security Center.

La utilidad klbackup se puede ejecutar en cualquiera de los siguientes modos:

- Interactivo
- No interactivo

## Copia de seguridad y recuperación de datos en modo interactivo

La restauración de los datos del Servidor de administración a partir de una copia de seguridad creada con la utilidad klbackup en modo interactivo puede producir un error. Si instaló el parche 15.1.0.20748-pf2 para el Servidor de administración y luego crea una copia de seguridad utilizando la utilidad klbackup con la opción **Migrar base de datos** deshabilitada, se produce un error al restaurar esta copia (para todos los DBMS, excepto MySQL y MariaDB). Si tiene instalado el parche 15.1.0.20748-pf2 para el Servidor de administración y desea crear una copia de seguridad sin migrar a otro DBMS, use una tarea de copia de seguridad de datos o ejecute la utilidad klbackup desde la línea de comando.

*Para crear una copia de seguridad de los datos del Servidor de administración en modo interactivo:*

1. Ejecute la utilidad klbackup ubicada en la carpeta de instalación de Kaspersky Security Center.

   Se inicia el Asistente de copias de seguridad y restauración.

2. En la primera ventana del asistente, seleccione **Realizar copia de seguridad de los datos del Servidor de administración**.

   Si marca la opción **Limitar la copia de seguridad o restauración al certificado del Servidor de administración**, sólo se guardará una copia de seguridad del certificado y la clave privada del Servidor de administración. La copia de seguridad del certificado y de la clave privada del Servidor de Administración puede ser útil cuando se realiza la migración desde el Servidor de Administración de Kaspersky Security Center Windows al Servidor de Administración de Kaspersky Security Center Linux. También puede migrar sus dispositivos administrados entre los distintos servidores de administración de Kaspersky Security Center Linux, así como entre distintos servidores de administración de Kaspersky Security Center Windows. Para obtener más información, consulte Uso de la utilidad klbackup para mover los dispositivos administrados y ponerlos bajo la administración de otro Servidor de administración.

   Haga clic en **Siguiente**.

3. En la siguiente ventana del Asistente, configure estos ajustes:

- **Carpeta de destino de la copia de seguridad**
- **Migrar base de datos**

  Habilite esta opción si actualmente almacena datos del Servidor de administración en una base de datos de Microsoft SQL Server y necesita migrarlos a una de las siguientes bases de datos: MySQL o MariaDB, PostgreSQL o Postgres Pro, Azure SQL. Esta opción está deshabilitada de forma predeterminada.

  - **Migrar al formato de MySQL/MariaDB**

    Habilite esta opción si el Servidor de administración utiliza SQL Server como DBMS y usted desea migrar los datos de SQL Server a un DBMS MySQL o MariaDB. Kaspersky Security Center creará una copia de seguridad compatible con MySQL y MariaDB. Podrá restaurar los datos de esa copia en MySQL o MariaDB.

  - **Migrar a Postgres**

    Habilite esta opción si el Servidor de administración utiliza SQL Server como DBMS y usted desea migrar los datos de SQL Server a un DBMS PostgreSQL o Postgres Pro. Kaspersky Security Center creará una copia de seguridad compatible con PostgreSQL y Postgres Pro. Después de eso, podrá restaurar los datos de la copia de seguridad en PostgreSQL o Postgres Pro.

    Esta opción estará disponible si envía una solitud al Soporte Técnico de Kaspersky e instala el parche 15.1.0.20748-pf2 para el Servidor de Administración o actualiza a Kaspersky Security Center Windows versión 15.1.0.22239.

  - **Migrar al formato de Azure**

    Habilite esta opción si el Servidor de administración utiliza SQL Server como DBMS y usted desea migrar los datos de SQL Server a un DBMS Azure SQL. Kaspersky Security Center creará una copia de seguridad compatible con Azure SQL. Podrá restaurar los datos de esa copia en Azure SQL.

- **Incluir la fecha y la hora actuales en el nombre de la carpeta de destino de la copia de seguridad**
- **Contraseña para la copia de seguridad**

4. Haga clic en el botón **Siguiente** para iniciar la copia de seguridad.

5. Si está trabajando con una base de datos en un entorno de nube como Amazon Web Services (AWS) o Microsoft Azure, en la ventana **Inicie sesión en el almacenamiento en línea**, rellene los siguientes campos:

   - Para AWS:

     - **Nombre del bucket de S3**

       El nombre del bucket de S3 que creó para la copia de seguridad.

     - **Id. de clave de acceso**

       Recibió el id. de clave (secuencia de caracteres alfanuméricos) cuando creó la cuenta de usuario de IAM para trabajar con la instancia de almacenamiento en buckets de S3.

       El campo está disponible si ha seleccionado la base de datos de RDS en un bucket de S3.

     - **Clave secreta**

       La clave secreta que recibió con el id. de la clave de acceso al crear la cuenta de usuario de IAM.

       Los caracteres de la clave secreta se muestran como asteriscos. Cuando comience a escribir la clave secreta, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado el tiempo que necesite para ver los caracteres introducidos.

       El campo está disponible si seleccionó una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

   - Para Microsoft Azure:

     - **Nombre de la cuenta de almacenamiento de Azure**

       Usted creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

     - **Id. de suscripción de Azure**

       Creó esta suscripción en el portal de Azure.

     - **Contraseña de Azure**

       Recibió la contraseña correspondiente al id. de aplicación cuando creó dicho id.

       Los caracteres de la contraseña se muestran como asteriscos. Cuando empiece a introducir la contraseña, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado para ver los caracteres introducidos.

     - **Id. de la aplicación en Azure**

Usted creó el id. de la aplicación en el portal de Azure.

No puede especificar más de un id. de aplicación de Azure para realizar sondeos u otros fines. Si desea sondear otro segmento de Azure, elimine primero la conexión de Azure existente.

- **Nombre del servidor SQL de Azure**

  El nombre y el grupo de recursos están disponibles en las propiedades del Servidor SQL de Azure.

- **Grupo de recursos del servidor SQL de Azure**

  El nombre y el grupo de recursos están disponibles en las propiedades del Servidor SQL de Azure.

- **Clave de acceso al almacenamiento de Azure**

  Disponible en las propiedades de su cuenta de almacenamiento, en la sección Claves de acceso. Puede utilizar cualquiera de las claves (key1 o key2).

*Para recuperar datos del Servidor de administración en modo interactivo:*

1. Ejecute la utilidad klbackup ubicada en la carpeta de instalación de Kaspersky Security Center. Para iniciar este programa, use la cuenta que haya usado al instalar el Servidor de administración. Le recomendamos que ejecute la utilidad en un Servidor de administración recientemente instalado.

   Se inicia el Asistente de copias de seguridad y restauración.

2. En la primera ventana del Asistente, seleccione **Restaurar datos del Servidor de administración** y luego haga clic en **Siguiente**.

   Si selecciona la opción **Limitar la copia de seguridad o restauración al certificado del Servidor de administración**, solo se recuperará el certificado del Servidor de administración.

   Cuando ejecute la utilidad klbackup en el nodo del clúster de conmutación por error inactivo, deberá seleccionar una de las siguientes opciones: especificar el certificado del Servidor de administración o recuperar datos automáticamente del Servidor de administración.

3. En la ventana **Opciones de restauración** del asistente, haga lo siguiente:

   - Especifique la carpeta que contiene una copia de seguridad de los datos del Servidor de administración.

     Si está utilizando un entorno de nube como AWS o Azure, indique la dirección del espacio de almacenamiento. Además, asegúrese de que el nombre del archivo sea backup.zip.

   - Especifique la contraseña que se ingresó durante la creación de la copia de seguridad de los datos.

     Al restaurar datos, debe especificar la misma contraseña que se ingresó durante la copia de seguridad. Si la ruta a una carpeta compartida se cambió después de la copia de seguridad, controle el funcionamiento de las tareas que usan los datos restaurados (tareas de restauración y tareas de instalación remota). Si es necesario, modifique la configuración de estas tareas. Mientras los datos se están restaurando desde una copia de seguridad, nadie debe acceder a la carpeta compartida del Servidor de administración. La cuenta desde la que se inicia la utilidad klbackup debe tener acceso completo a la carpeta compartida.

4. Haga clic en el botón **Siguiente** para restaurar los datos.

## Copia de seguridad y recuperación de datos en modo no interactivo

*Para crear una copia de seguridad o recuperar los datos del Servidor de administración en modo no interactivo,*

En el dispositivo del Servidor de administración, abra la línea de comandos y ejecute klbackup con las claves necesarias.

Los indicadores del Agente de red no se restauran cuando se utiliza la utilidad klbackup. Debe configurar los indicadores del Agente de red manualmente.

La instancia del Servidor de Administración en la que se va a realizar la restauración debe utilizar un DBMS del mismo tipo. La versión del Servidor de administración puede ser igual (con un parche idéntico o posterior) o posterior.

Sintaxis de línea de comandos de la utilidad:

```
klbackup -path <backup path> [-linux_path <ruta de copia de seguridad de SQL Server>][-
node_cert <ruta del certificado>] [-logfile <archivo de registro>] [-use_ts]|[-
restore] [-password <contraseña>] [-cert_only] [-online] [-migrate postgres]
```

Si no se especificó una contraseña en la línea de comandos de la utilidad klbackup, la utilidad solicitará que se ingrese la contraseña de modo interactivo.

Descripciones de las claves:

- `-path <ruta de respaldo>`: guardar información en la carpeta de respaldo o usar datos de la carpeta de respaldo para la recuperación (parámetro obligatorio).

  La cuenta del servidor de bases de datos y la utilidad klbackup deben contar con permisos para modificar los datos de la carpeta de la copia de seguridad.

- `-linux_path <ruta de respaldo de SQL Server>`: ruta local a la carpeta con datos de respaldo para SQL Server en Linux.

  La cuenta del servidor de bases de datos y la utilidad klbackup deben contar con permisos para modificar los datos de la carpeta de respaldo de SQL Server.

- `-node_cert <ruta al certificado>`: archivo de certificado del servidor para configurar el nodo del clúster de conmutación por error inactivo después de la recuperación. Si no se configura, se recuperará automáticamente del Servidor.

  Al ejecutar la utilidad klbackup en el nodo del clúster de conmutación por error inactivo, use esta clave para especificar la ruta al certificado del servidor.

- `-logfile <archivo de registro>`: guardar un informe sobre la copia de seguridad y recuperación de datos del Servidor de administración.

- `-use_ts`: al guardar datos, copie la información a la carpeta de la copia de seguridad, a la subcarpeta con un nombre en el formato `klbackup AAAA-MM-DD # HH-MM-SS`, que incluye la fecha actual y la hora de funcionamiento en UTC. Si no se especifica una clave, la información se guarda en la raíz de la carpeta de la copia de seguridad.

  Durante los intentos de guardar información en una carpeta que ya contiene una copia de seguridad, aparece un mensaje de error. No se actualiza la información.

  La disponibilidad de la clave `-use_ts` permite mantener un archivo de datos del Servidor de administración. Por ejemplo, si la clave `-path` indica la carpeta `C:\KLBackups`, entonces la carpeta `klbackup 2022/6/19 # 11-30-18` almacena información sobre el estado del Servidor de administración con fecha de 19 de junio de 2022, a las 11:30:18 h.

- `-restore`: recuperar datos del Servidor de Administración. La recuperación de los datos se realiza a partir de la información almacenada en la carpeta de la copia de seguridad. Si no se dispone de una clave, se crea una copia de seguridad de los datos en la carpeta de la copia de seguridad.

- `-password <contraseña>`: contraseña para proteger los datos confidenciales.

  > Si olvida la contraseña, no podrá recuperarla. No hay requisitos para la contraseña. La longitud de la contraseña es ilimitada y también es posible que tenga una longitud cero (es decir, sin contraseña).

  Al restaurar datos, debe especificar la misma contraseña que se ingresó durante la copia de seguridad. Si la ruta a una carpeta compartida se cambió después de la copia de seguridad, controle el funcionamiento de las tareas que usan los datos restaurados (tareas de restauración y tareas de instalación remota). Si es necesario, modifique la configuración de estas tareas. Mientras los datos se están restaurando desde una copia de seguridad, nadie debe acceder a la carpeta compartida del Servidor de administración. La cuenta desde la que se inicia la utilidad klbackup debe tener acceso completo a la carpeta compartida. Recomendamos que ejecute la utilidad en un Servidor de administración recién instalado.

- `-cert_only`: guardar o recuperar solo el certificado y la clave privada del Servidor de administración.

  Este indicador puede ser útil cuando realiza la migración desde el Servidor de administración de Kaspersky Security Center Windows al Servidor de administración de Kaspersky Security Center Linux. Además, puede migrar dispositivos administrados entre los Servidores de administración de Kaspersky Security Center Linux, así como entre los Servidores de administración de Kaspersky Security Center Windows.

- `-online`: Para generar la copia de seguridad, crear una instantánea del volumen. Con ello se minimiza el tiempo de inactividad del Servidor de administración. Esta opción no tiene ningún efecto cuando la utilidad se emplea en modo de recuperación. No utilice este indicador al crear una copia de seguridad para migrar a un DBMS diferente.

- `-archive 0`: mantiene los datos del servidor como archivos sin formato. Por defecto (`-archive 1`), los datos del servidor se guardan en un archivo de almacenamiento.

- `-migrate mysql`: cree una copia de seguridad de los datos del Servidor de administración almacenados en la base de datos de SQL Server que es compatible con MySQL (incluido MariaDB). Puede restaurar los datos de esa copia en MySQL.

- `-migrate postgres`: cree una copia de seguridad de los datos del Servidor de administración almacenados en la base de datos de SQL Server que es compatible con PostgreSQL y Postgres Pro. Puede restaurar los datos de la copia de seguridad en PostgreSQL o Postgres Pro. Utilice este indicador cuando realice la migración a Kaspersky Security Center Linux mediante la copia de seguridad de los datos del Servidor de administración.

  Esta opción estará disponible si envía una solicitud al Soporte Técnico de Kaspersky e instala el parche 15.1.0.20748-pf2 para el Servidor de Administración o actualiza a Kaspersky Security Center Windows versión 15.1.0.22239.

## Usar la utilidad klbackup para ceder el control de los dispositivos administrados a otro Servidor de administración

La utilidad klbackup permite ceder el control de los dispositivos administrados a otro Servidor de administración Puede cambiar el Servidor de administración de Kaspersky Security Center Windows por el Servidor de administración de Kaspersky Security Center Linux mediante la utilidad klbackup tras completar la migración. También puede migrar sus dispositivos administrados entre los distintos servidores de administración de Kaspersky Security Center Linux, así como entre distintos servidores de administración de Kaspersky Security Center Windows.

*Para ceder el control de un grupo de dispositivos administrados a otro Servidor de administración mediante la utilidad klbackup:*

1. En el dispositivo antiguo, cree una copia de seguridad del certificado y de la clave privada del Servidor de administración.

   Puede crear una copia de seguridad de distintas maneras:

   - Mediante la interfaz de la utilidad klbackup (solo para el Servidor de administración de Kaspersky Security Center Windows)

     Ejecute la utilidad klbackup ubicada en la carpeta de instalación de Kaspersky Security Center y luego cree una copia de seguridad usando la opción **Limitar la copia de seguridad o restauración al certificado del Servidor de administración**.

   - Mediante la línea de comandos (para Kaspersky Security Center Windows y servidores de administración de Kaspersky Security Center Linux versión 15.1 o versiones posteriores)

     Ejecute la utilidad klbackup con la clave `-cert_only` desde la línea de comandos para crear una copia de seguridad del certificado y de la clave privada del Servidor de administración:

     ```
     klbackup -path <ruta a la copia de seguridad del certificado del Servidor de Administración> -cert_only
     ```

2. En el dispositivo antiguo, desconecte el Servidor de administración de la red.

3. Asigne la misma dirección al dispositivo que contenga el otro Servidor de administración.

   Al nuevo Servidor de Administración se le puede asignar un nombre NetBIOS, un FQDN y una dirección IP estática. Esto depende de la dirección del Servidor de administración que se haya configurado en el paquete de instalación del Agente de red cuando se desplegaron los agentes de red. Como alternativa, puede usar la dirección de conexión que determina el Servidor de administración al que se conecta el Agente de red (puede obtener esta dirección en los dispositivos administrados mediante la utilidad klnagchk).

4. En el dispositivo con el otro Servidor de administración, utilice la copia de seguridad para restaurar el certificado y la clave privada del Servidor de administración.

   Puede restaurar una copia de seguridad de distintas maneras:

   - Mediante la interfaz de la utilidad klbackup (solo para el Servidor de administración de Kaspersky Security Center Windows)

     Ejecute la utilidad klbackup y luego restaure la copia de seguridad usando la opción **Limitar la copia de seguridad o restauración al certificado del Servidor de administración**.

   - Mediante la línea de comandos (para Kaspersky Security Center Windows y servidores de administración de Kaspersky Security Center Linux versión 15.1 o versiones posteriores)

     Ejecute la utilidad klbackup con la clave `-cert_only` desde la línea de comandos para restaurar una copia de seguridad del certificado del Servidor de administración y de la clave privada:

     ```
     klbackup -path <ruta a la copia de seguridad del certificado del Servidor de Administración> -restore -cert_only
     ```

Los dispositivos administrados quedarán bajo la órbita administrativa del otro Servidor de administración. Puede ir a este Servidor de administración y asegurarse de que los dispositivos administrados sean visibles en la red y que el Agente de red esté instalado y activo en ellos (las columnas **Visible**, **Agente de red instalado** y **Agente de red en ejecución** deben tener el valor *Sí*).

## Cómo hacer copias de seguridad y restaurar datos del Servidor de administración si se usa MySQL o MariaDB

Puede utilizar una copia de seguridad para migrar los datos del Servidor de administración de Kaspersky Security Center Windows y ponerlos bajo la órbita administrativa de Kaspersky Security Center Linux. La migración con una copia de seguridad de datos solo se admite para la migración a Kaspersky Security Center Linux 15.2 o versiones posteriores desde cualquier versión compatible de Kaspersky Security Center Windows.

Si utiliza MySQL o MariaDB como DBMS para Kaspersky Security Center Windows y Kaspersky Security Center Linux, el parámetro `lower_case_table_names` debe ser el mismo en el DBMS activo y el nuevo. De lo contrario, los datos del Servidor de administración se migrarán incorrectamente.

Antes de realizar una copia de seguridad de los datos del Servidor de administración en Kaspersky Security Center Windows, controle el valor del parámetro `lower_case_table_names`. Si no definió este parámetro durante la instalación del DBMS, se utilizará el valor predeterminado para el parámetro. El valor predeterminado del parámetro `lower_case_table_names` para Windows es `1`.

Al instalar MySQL o MariaDB para Kaspersky Security Center Linux, asigne al parámetro `lower_case_table_names` el mismo valor que se haya definido para él en Windows; siga para ello las instrucciones en el sitio web de MySQL. Si no especifica este parámetro, se utilizará el valor predeterminado para el mismo. En sistemas operativos Linux, el valor predeterminado del parámetro `lower_case_table_names` es diferente del valor predeterminado en Windows.

Si desea instalar MySQL 8.0, definir el parámetro `lower_case_table_names` siguiendo estas instrucciones puede no dar el resultado esperado. En tal caso, primero instale MySQL 5.7, defina el parámetro `lower_case_table_names` siguiendo las instrucciones y luego actualice MySQL 5.7 a MySQL 8.0. Si el parámetro `lower_case_table_names` no es el mismo en el DBMS activo y el nuevo, los datos del Servidor de administración no se restaurarán correctamente.

## Optimizar la copia de seguridad y restauración de los datos del Servidor de administración

*Para optimizar la copia de seguridad y la restauración de los datos del Servidor de administración para reducir el tiempo de inactividad del Servidor de administración, lleve a cabo una de las siguientes acciones:*

- Active la opción **Usar instantánea del sistema de archivos para la copia de seguridad de datos**.

  Consulte el siguiente artículo para obtener más información: Uso de una instantánea del sistema de archivos para reducir la duración de la copia de seguridad.

- Configure los siguientes indicadores:

  Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada es <Disk>:\Archivos de programa(x86)\Kaspersky Lab\Kaspersky Security Center.

  - `KLSRV_BKP_FILES`: divide el archivo de base de datos en varios archivos más pequeños, de 2 a 32. Esto puede acelerar la copia de seguridad y la restauración si el rendimiento del DBMS está limitado por la CPU.

    Ejemplo:

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_FILES -t d -v 2
    ```

  - `KLSRV_BKP_BACKUP_EXTRA_PARS`: especifica los parámetros `COMPRESSION` y `MAXTRANSFERSIZE`. Esto puede acelerar la copia de seguridad si el rendimiento del DBMS tiene límites de entrada o salida de archivos.

    Ejemplo:

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_BACKUP_EXTRA_PARS -t s -v "COMPRESSION,
    MAXTRANSFERSIZE = 4194304"
    ```

  - `KLSRV_BKP_RESTORE_EXTRA_PARS`: especifica el parámetro `MAXTRANSFERSIZE`. Esto puede acelerar la restauración de la copia de seguridad si el rendimiento del DBMS tiene límites de entrada o salida de archivos.

    Ejemplo:

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_RESTORE_EXTRA_PARS -t s -v "MAXTRANSFERSIZE
    = 4194304"
    ```

  - `KLSRV_BKP_ONLINE_DB_BACKUP`: elimina el tiempo de inactividad del Servidor de administración durante la copia de seguridad. Sólo disponible para los siguientes DBMS:

    - PostgreSQL o Postgres Pro.
    - SQL Server con el modelo de recuperación completa. Consulte la documentación de SQL Server para obtener más detalles. Cuando habilita el indicador `KLSRV_BKP_ONLINE_DB_BACKUP`, el DBMS de SQL Server cambia automáticamente al modelo de recuperación completa.

    Ejemplo:

    ```
    klscflag.exe -fset -pv klserver -n KLSRV_BKP_ONLINE_DB_BACKUP -t d -v 1
    ```

# Mover el Servidor de administración a otro dispositivo

Si necesita usar el Servidor de administración en un nuevo dispositivo, puede moverlo de una de las siguientes maneras:

- Mueva el Servidor de administración y el servidor de la base de datos a un nuevo dispositivo (el servidor de la base de datos se puede instalar en el nuevo dispositivo junto con el Servidor de administración, o en otro dispositivo).
- Mantenga el servidor de la base de datos en el dispositivo anterior y mueva solo el Servidor de administración a un nuevo dispositivo.

*Para mover el Servidor de administración a un nuevo dispositivo, haga lo siguiente:*

1. En el dispositivo anterior, cree una copia de seguridad de los datos del Servidor de administración.

   Para ello, inicie la tarea de copia de seguridad de datos a través de la Consola de administración o ejecute la utilidad klbackup.

   Habilite esta opción si el Servidor de administración utiliza SQL Server como DBMS y usted desea migrar los datos de SQL Server a un DBMS MySQL o MariaDB. Para hacer esto, ejecute la utilidad klbackup en modo interactivo para crear una copia de seguridad de los datos. Habilite la opción **Migrar al formato de MySQL/MariaDB** en el la ventana **Opciones de copia de seguridad** del asistente de copias de seguridad y restauración. Kaspersky Security Center creará una copia de seguridad compatible con MySQL y MariaDB. Podrá restaurar los datos de esa copia en MySQL o MariaDB.

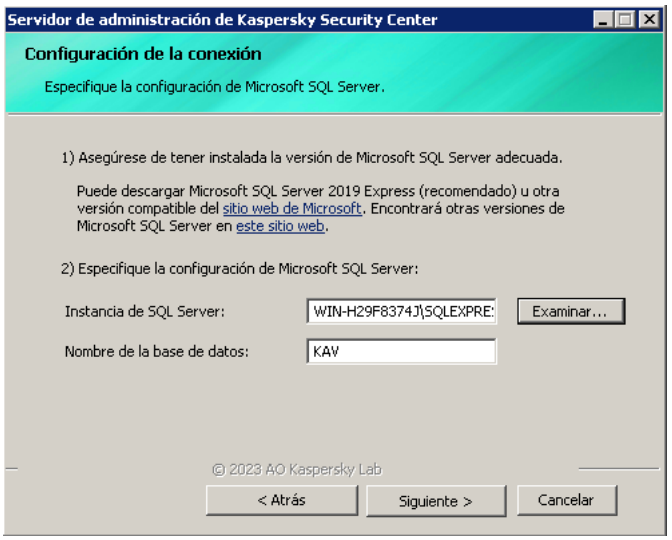
   También puede habilitar la opción **Migrar al formato de Azure** si desea migrar los datos de SQL Server a Azure SQL DBMS.

2. En el dispositivo anterior, desconecte el Servidor de administración de la red.
3. Seleccione un nuevo dispositivo para instalar el Servidor de administración. Asegúrese de que el hardware y el software del dispositivo seleccionado cumplan con los requisitos del Servidor de administración, de la Consola de administración y del Agente de red. Además, compruebe que haya puertos utilizados en el Servidor de administración disponibles.
4. Asigne la misma dirección al nuevo dispositivo.

   Al nuevo Servidor de Administración se le puede asignar un nombre NetBIOS, un FQDN y una dirección IP estática. Esto depende de la dirección del Servidor de administración que se haya configurado en el paquete de instalación del Agente de red cuando se desplegaron los agentes de red. Como alternativa, puede usar la dirección de conexión que determina el Servidor de administración al que se conecta el Agente de red (puede obtener esta dirección en los dispositivos administrados mediante la utilidad klnagchk).
5. Si es necesario, instale en otro dispositivo el sistema de administración de base de datos (DBMS) que utilizará el Servidor de administración.

   La base de datos se puede instalar en el nuevo dispositivo junto con el Servidor de administración o en otro dispositivo. Cerciórese de que este dispositivo cumpla con los requisitos de hardware y software. Cuando seleccione un DBMS, tenga en cuenta la cantidad de dispositivos cubiertos por el Servidor de administración.
6. Ejecute la instalación del Servidor de administración en el nuevo dispositivo.

7. Durante la instalación del Servidor de administración, configure los parámetros de conexión del servidor de la base de datos.




Ejemplo de la ventana de configuración de conexión para Microsoft SQL Server

Dependiendo de dónde necesite ubicar el servidor de la base de datos, realice una de las siguientes acciones:

- Mantenga el servidor de la base de datos en el dispositivo anterior

  1. Haga clic en el botón **Examinar** junto al campo **Instancia de SQL Server** y seleccione el nombre del dispositivo anterior en la lista que aparece.

     Tenga en cuenta que el dispositivo anterior debe estar disponible para la conexión con el nuevo Servidor de Administración.

  2. Introduzca el nombre de la base de datos anterior en el campo **Nombre de la base de datos**.

- Mueva el servidor de la base de datos a otro dispositivo

  1. Haga clic en el botón **Examinar** junto al campo **Instancia de SQL Server** y seleccione el nuevo nombre del dispositivo en la lista que aparece.

  2. Introduzca el nuevo nombre de la base de datos en el campo **Nombre de la base de datos**.

     Tenga en cuenta que el nuevo nombre de la base de datos debe coincidir con el nombre de la base de datos del dispositivo anterior. Los nombres de las bases de datos deben ser idénticos para que se pueda utilizar la copia de seguridad del Servidor de administración. El nombre predeterminado de la base de datos es *KAV*.

8. Una vez completada la instalación, recupere los datos del Servidor de administración en el nuevo dispositivo mediante la utilidad klbackup.

   Si utiliza SQL Server como DBMS en los dispositivos anteriores y nuevos, tenga en cuenta que la versión de SQL Server instalada en el dispositivo nuevo debe ser igual o posterior a la versión de SQL Server instalada en el dispositivo anterior. De lo contrario, no podrá recuperar los datos del Servidor de administración en el dispositivo nuevo.

9. Abra la consola de administración y conéctese al Servidor de administración.

10. Verifique que todos los dispositivos administrados estén conectados al Servidor de administración.

11. Desinstale el Servidor de administración y el servidor de la base de datos del dispositivo anterior.

También puede usar Kaspersky Security Center Web Console para mover el Servidor de administración y un servidor de bases de datos a otro dispositivo.

## Evitar conflictos entre varios Servidores de administración

Si tiene más de un Servidor de administración en su red, pueden ver los mismos dispositivos cliente. Esto puede resultar, por ejemplo, en que el Servidor de administración instale una aplicación que ya fue instalada por otro Servidor de administración, y otros tipos de conflictos. Para evitar que una aplicación se instale en un dispositivo administrado por otro Servidor de administración, debe habilitar la opción **Instalar solo en dispositivos administrados a través de este Servidor de administración** en las propiedades de la tarea *Instalar aplicación de forma remota*.

Si habilita la opción **Instalar solo en dispositivos administrados a través de este Servidor de administración** y luego ejecuta la tarea *Instalar aplicación de forma remota*, se realiza una verificación para determinar si los dispositivos están administrados por otro Servidor de administración. Para los dispositivos administrados por otro Servidor de administración, el valor del atributo **Administrado por un Servidor de administración diferente** se establecerá en `true`. La tarea *Instalar aplicación de forma remota* no se aplicará a estos dispositivos.

Los valores del atributo **Administrado por un Servidor de administración diferente** se muestran en la columna **Administrado por un Servidor de administración diferente** en la lista de dispositivos administrados y la lista de dispositivos no asignados.

También puede usar la propiedad **Administrado por un Servidor de administración diferente** como criterio para los siguientes propósitos:

- Búsqueda de dispositivos
- Selecciones de dispositivos
- Reglas de movimiento de dispositivos
- Reglas de etiquetado automático

*Para restablecer el atributo Administrado por un Servidor de administración diferente:*

1. En el menú principal de Kaspersky Security Center Web Console, vaya a **Descubrimiento y despliegue → Dispositivos no asignados**.

2. Seleccione el dispositivo requerido y, a continuación, haga clic en el botón **Eliminar el atributo Administrado por un Servidor de administración diferente**.

Se restablece el atributo **Administrado por un Servidor de administración diferente**.

# Administrar grupos de administración

Esta sección proporciona información sobre cómo administrar grupos de administración.

Se pueden realizar las siguientes acciones en los grupos de administración:

- Agregar cualquier número de grupos anidados de cualquier nivel de jerarquía a los grupos de administración.
- Agregar dispositivos a grupos de administración.
- Cambiar la jerarquía de los grupos de administración moviendo los dispositivos individuales y los grupos enteros a otros grupos.
- Eliminar los grupos anidados y los dispositivos de los grupos de administración.
- Agregar Servidores de administración secundarios y virtuales a los grupos de administración.
- Mover los dispositivos de los grupos de administración de un Servidor de administración a los de otro Servidor.
- Definir qué aplicaciones de Kaspersky serán automáticamente instaladas en los dispositivos incluidos en un grupo.

Puede realizar estas acciones solo si tiene el permiso **Modificar** en el área **Administración de grupos de administración** para los grupos de administración que desea administrar (o para el Servidor de administración al que pertenecen estos grupos).

## Creación de grupos de administración

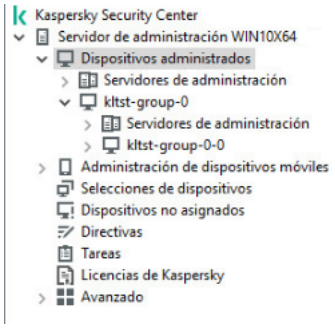
La jerarquía de grupos de administración se crea en la ventana principal de la aplicación de Kaspersky Security Center, en la carpeta **Dispositivos administrados**. Los grupos de administración se muestran como carpetas en el árbol de consola (ver la figura a continuación).

Inmediatamente después de la instalación de Kaspersky Security Center, la carpeta **Dispositivos administrados** contendrá únicamente una carpeta vacía **Servidores de administración**.

> La configuración de la interfaz de usuario determina si la carpeta **Servidores de administración** aparece o no en el árbol de consola. Para mostrar esta carpeta, en la barra del menú, seleccione **Ver → Configuración de interfaz** y en la ventana **Configuración de interfaz** que se abre seleccione la casilla **Mostrar Servidores de administración secundarios**.

Al crear una jerarquía de grupos de administración, puede agregar dispositivos y máquinas virtuales a la carpeta **Dispositivos administrados**, y también puede agregar grupos anidados. Puede agregar Servidores de administración secundarios y virtuales a la carpeta **Servidores de administración**.

Al igual que con la carpeta **Dispositivos administrados**, cada grupo creado inicialmente contiene solo la carpeta **Servidores de administración**, que está vacía y que sirve para trabajar con los Servidores de administración secundarios y virtuales de este grupo. La información sobre las directivas y tareas de este grupo, y la información sobre los dispositivos incluidos en este grupo, se muestra en las pestañas con los nombres correspondientes en el espacio de trabajo de este grupo.




Ver jerarquía de grupos de administración

*Para crear un grupo de administración:*

1. En el árbol de consola, expanda la carpeta **Dispositivos administrados**.
2. Si desea crear un subgrupo para un grupo de administración existente, en la carpeta **Dispositivos administrados** seleccione la subcarpeta que corresponde al grupo, que debería incluir el nuevo grupo de administración.

   Puede omitir este paso si crea un nuevo grupo de administración de nivel superior.
3. Inicie la creación del grupo de administración de una de las siguientes formas:

   - Utilice el comando **Crear → Grupo** en el menú contextual.
   - Haga clic en el botón **Nuevo grupo** que se encuentra en el espacio de trabajo de la ventana principal de la aplicación, en la pestaña **Dispositivos**.
4. En la ventana **Nombre de grupo** que se abre, escriba un nombre para el grupo y haga clic en **Aceptar**.

Aparece una nueva carpeta de grupo de administración con el nombre especificado en el árbol de consola.

La aplicación permite crear una jerarquía de grupos de administración basada en la estructura de Active Directory o en la estructura de la red del dominio. También es posible crear una estructura de grupos a partir de un archivo de texto.

*Para crear una estructura de grupos de administración:*

1. En el árbol de consola, seleccione la carpeta **Dispositivos administrados**.
2. En el menú contextual de la carpeta **Dispositivos administrados**, seleccione **Todas las tareas → Nueva estructura de grupo**.

Se inicia el Asistente de nueva estructura de grupos de administración. Siga las instrucciones del asistente.

## Traslado de grupos de administración

Puede mover grupos de administración anidados dentro de la jerarquía de grupos.

Un grupo de administración se mueve junto con todos sus grupos anidados, Servidores de administración secundarios, dispositivos, directivas de grupo y tareas. El sistema aplicará al grupo toda la configuración correspondiente a su nueva posición en la jerarquía de los grupos de administración.

El nombre del grupo debe ser único dentro de un nivel de la jerarquía. Si ya existe un grupo con el mismo nombre en la carpeta a la que se mueve el grupo de administración, debe cambiar el nombre de este último. Si no cambió el nombre del grupo que se moverá, cuando lo mueva, automáticamente se agregará un índice en formato **(<siguiente número de la secuencia>)** al nombre, por ejemplo: **(1)**, **(2)**.

No se puede cambiar el nombre al grupo **Dispositivos administrados** porque es un elemento integrado de la Consola de administración.

*Para mover un grupo a otra carpeta del árbol de consola:*

1. Seleccione un grupo para mover en el árbol de consola.
2. Realice una de las siguientes acciones:
   - Mueva el grupo mediante el menú contextual:
     1. Seleccione **Cortar** en el menú contextual del grupo.
     2. Seleccione **Pegar** en el menú contextual del grupo de administración al que desea mover el grupo seleccionado.
   - Mueva el grupo mediante el menú principal de la aplicación:
     a. En el menú principal, seleccione **Acción** → **Cortar**.
     b. En el árbol de consola, seleccione el grupo de administración al que necesita mover en el grupo seleccionado.
     c. En el menú principal, seleccione **Acción** → **Pegar**.
   - Con el mouse, mueva el grupo a otro en el árbol de consola.

## Eliminación de grupos de administración

Se puede eliminar un grupo de administración si no contiene Servidores de administración secundarios, grupos anidados o dispositivos cliente y si no se han creado tareas o directivas de grupo.

Antes de eliminar el grupo de administración, debe eliminar todos los Servidores de administración secundarios, grupos anidados y dispositivos cliente de ese grupo.

*Para eliminar un grupo:*

1. Seleccione un grupo de administración del árbol de consola.
2. Realice una de las siguientes acciones:
   - Seleccione **Eliminar** en el menú contextual del grupo.
   - En el menú principal de la aplicación, seleccione **Acción → Eliminar**.
   - Pulse la tecla **SUPRIMIR**.

## Creación automática de la estructura de grupos de administración

Kaspersky Security Center le permite crear una estructura de grupos de administración mediante el Asistente de creación de jerarquía de grupos.

El asistente crea una estructura de grupo de administración basada en los siguientes datos:

- Estructuras de dominios de Windows y grupos de trabajo
- Estructuras de grupos del Active Directory
- Contenido de un archivo de texto creado manualmente por el administrador

Cuando el archivo de texto se genera, se deben cumplir los requisitos siguientes:

- El nombre de cada grupo nuevo debe comenzar con una nueva línea; el separador debe comenzar con un fin de línea. Se ignoran las líneas en blanco.

  Ejemplo:
  Oficina 1
  Oficina 2
  Oficina 3
  Se deben crear tres grupos del primer nivel de jerarquía en el grupo de destino.

- El nombre del grupo anidado se debe ingresar con una barra diagonal (/).

  Ejemplo:
  Oficina 1/División 1/Departamento 1/Grupo 1
  Se crearán cuatro subgrupos anidados en cada uno, en el grupo de destino.

- Para crear varios grupos anidados del mismo nivel de jerarquía, debe especificar la "ruta completa al grupo".

  Ejemplo:
  Oficina 1/División 1/Departamento 1
  Oficina 1/División 2/Departamento 1
  Oficina 1/División 3/Departamento 1
  Oficina 1/División 4/Departamento 1
  Un grupo de la Oficina 1 del primer nivel de jerarquía deberá ser creado en el grupo de destino. Este grupo incluirá cuatro grupos anidados del mismo nivel de jerarquía: "División 1", "División 2", "División 3" y "División 4". Cada uno de estos grupos incluirá el grupo "Departamento 1".

La creación de la jerarquía de grupos de administración a través del asistente no afecta la integridad de la red: en vez de grupos existentes reemplazados, los grupos nuevos se agregan. Un dispositivo cliente no se puede incluir en un grupo de administración una segunda vez porque el dispositivo se elimina desde el grupo **Dispositivos no asignados** cuando se mueve al grupo de administración.

Si, al crear la estructura del grupo de administración, un dispositivo no se incluyó en el grupo **Dispositivos no asignados** por la razón que sea (se apagó o se desconectó de la red), no se moverá automáticamente al grupo de administración. Puede agregar manualmente dispositivos a los grupos de administración luego de que el asistente concluya su operación.

*Para iniciar la creación automática de la estructura de grupos de administración:*

1. Seleccione la carpeta **Dispositivos administrados** en el árbol de consola.
2. En el menú contextual de la carpeta **Dispositivos administrados**, seleccione **Todas las tareas → Nueva estructura de grupo**.

Se inicia el Asistente de nueva estructura de grupos de administración. Siga las instrucciones del asistente.

## Instalación automática de aplicaciones en dispositivos de un grupo de administración

Puede especificar qué paquetes de instalación deben utilizarse para la instalación remota automática de aplicaciones Kaspersky en dispositivos cliente de un grupo de administración.

*Para configurar la instalación automática de las aplicaciones en dispositivos nuevos de un grupo de administración:*

1. En el árbol de consola, seleccione el grupo de administración requerido.
2. Abra la ventana de propiedades de este grupo de administración.
3. En el panel **Secciones**, seleccione **Instalación automática** y, en el espacio de trabajo, seleccione los paquetes de instalación de las aplicaciones que se instalarán en los dispositivos.
4. Haga clic en **Aceptar**.

Se crean tareas de grupo. Estas tareas se ejecutan en los dispositivos cliente inmediatamente después de que se agregan al grupo de administración.

Si se seleccionaran varios paquetes de instalación de una aplicación para la instalación automática, la tarea de instalación se creará solamente para la versión más reciente de la aplicación.

# Administración de dispositivos cliente

Esta sección contiene la información sobre el funcionamiento con dispositivos cliente.

# Conexión de dispositivos cliente al Servidor de administración

La conexión del dispositivo cliente al Servidor de administración se establece a través del Agente de red instalado en el dispositivo cliente.

Cuando un dispositivo cliente se conecta al Servidor de administración, se realizan las siguientes operaciones:

- Sincronización automática de datos:
  - La sincronización de la lista de aplicaciones instalada en el dispositivo cliente.
  - Sincronización de las directivas, configuración de la aplicación, tareas y configuración de la tarea.
- Recuperación de información actualizada sobre la condición de las aplicaciones, ejecución de tareas y estadísticas de funcionamiento de aplicaciones a través del Servidor de administración.
- Envío de la información sobre eventos al Servidor de administración para su procesamiento.

La sincronización automática de datos se realiza regularmente, de acuerdo con la configuración del Agente de red (por ejemplo, cada 15 minutos). Puede especificar el intervalo de conexión manualmente.

La información sobre un evento se envía al Servidor de administración inmediatamente después de producirse el evento.

Si un Servidor de administración está ubicado fuera de una red corporativa, los dispositivos cliente se conectarán a este a través de Internet.

Para que los dispositivos se conecten a un Servidor de administración a través de Internet, se deben cumplir las siguientes condiciones:

- El Servidor de administración remota debe tener una dirección IP externa y el puerto entrante 13000 debe permanecer abierto (para la conexión de los agentes de red). Le recomendamos que también abra el puerto UDP 13000 (para recibir notificaciones de apagado del dispositivo).
- Primero deben instalarse los Agentes de red en los dispositivos.
- Al instalar el Agente de red en dispositivos, debe especificar la dirección IP externa del Servidor de administración remoto. Si se utiliza un paquete de instalación para la instalación, la dirección IP externa se debe especificar manualmente en las propiedades de este paquete, en la sección **Configuración**.
- Para usar el Servidor de administración remoto con el fin de administrar las aplicaciones y tareas de un dispositivo, en la ventana de propiedades de ese dispositivo, en la sección **General**, seleccione la casilla **No desconectar del Servidor de administración**. Una vez que la casilla está seleccionada, espere a que el Servidor de administración esté sincronizado con el dispositivo remoto. El número de dispositivos cliente que mantienen una conexión continua con un Servidor de administración remoto no puede superar los 300.

Para acelerar el rendimiento de las tareas generadas por un Servidor de administración remoto, puede abrir el puerto 15000 en un dispositivo. En este caso, para ejecutar una tarea, el Servidor de administración envía un paquete especial al Agente de red a través del puerto 15000 sin esperar a que se complete la sincronización con el dispositivo.

Kaspersky Security Center le permite configurar la conexión entre un dispositivo cliente y un Servidor de administración de modo que la conexión permanezca activa una vez que se completaron todas las operaciones. La conexión ininterrumpida es necesaria en casos en que se requiere supervisión en tiempo real del estado de la aplicación y el Servidor de administración no sea capaz de establecer una conexión con el cliente por algún motivo (conexión protegida por firewall, no se permite abrir puertos en el dispositivo cliente, dirección IP del dispositivo cliente desconocida, etc.). Se puede establecer una conexión ininterrumpida entre un dispositivo cliente y el Servidor de administración en la ventana de propiedades del dispositivo cliente, en la sección **General**.

Recomendamos establecer una conexión ininterrumpida con los dispositivos más importantes. El número total de conexiones mantenidas simultáneamente por el Servidor de administración está limitado a 300.

Al sincronizar manualmente, el sistema utiliza un método de conexión auxiliar, con el cual la conexión es iniciada por el Servidor de administración. Antes de establecer la conexión en un dispositivo cliente, debe abrir el puerto UDP. El Servidor de administración envía una solicitud de conexión al puerto UDP del dispositivo cliente. En respuesta, se verifica el certificado del Servidor de administración. Si el certificado del Servidor de administración coincide con la copia del certificado almacenada en el dispositivo cliente, se establece la conexión.

El inicio manual de la sincronización también se utiliza para obtener información actualizada sobre la condición de las aplicaciones, la ejecución de tareas y las estadísticas de operación de las aplicaciones.

## Conexión manual de un dispositivo cliente al Servidor de administración. Utilidad klmover

Si desea conectar un dispositivo cliente al Servidor de administración, puede utilizar la utilidad klmover en el dispositivo cliente.

Al instalar el Agente de red en un dispositivo cliente, la utilidad se copia automáticamente a la carpeta de instalación del Agente de red.

*Para conectar manualmente un dispositivo cliente al Servidor de administración mediante la utilidad klmover:*

En el dispositivo, inicie la utilidad klmover desde la línea de comandos.

Al iniciarse desde la línea de comandos, la utilidad klmover puede realizar las siguientes acciones (dependiendo de las claves en uso):

- Conecta el Agente de red al Servidor de administración con la configuración especificada.
- Registra los resultados de la operación en el archivo de registro del evento o los muestra en pantalla.

No se puede utilizar la utilidad klmover para dispositivos cliente conectados al Servidor de administración mediante puertas de enlace de conexión. Para estos dispositivos, debe reconfigurar el Agente de red o reinstalar el Agente de red y especificar la puerta de enlace de conexión.

Sintaxis de línea de comandos de la utilidad:

```
klmover [-logfile <nombre de archivo>] [-address <dirección del servidor>] [-pn
<número de puerto>] [-ps <número de puerto SSL>] [-nossl] [-cert <ruta al archivo de
certificado>] [-silent] [-dupfix] [-virtserv] [-cloningmode]
```

Se requieren derechos de administrador para ejecutar la utilidad.

Descripciones de las claves:

- `-logfile <file name>`: registra los resultados de ejecución de la utilidad en un archivo de registro.

  De manera predeterminada, la información se guarda en el flujo saliente estándar (stdout). Si la clave no está en uso, los resultados y mensajes de error se muestran en pantalla.

- `-address <server address>`: la dirección del Servidor de administración para la conexión.

  Puede especificar como dirección una dirección IP, el nombre NetBIOS o el nombre DNS de los dispositivos.

- `-pn <port number>`: número del puerto a través del cual se establecerá la conexión no cifrada al Servidor de administración.

  El número de puerto predeterminado es 14000.

- `-ps <SSL port number>`: número del puerto SSL a través del cual se establece la conexión al Servidor de administración, utilizando SSL.

  El número de puerto predeterminado es 13000.

- `-nossl`: usar conexión no cifrada al Servidor de administración.

  Si la clave no está en uso, el Agente de red se conecta al Servidor de administración mediante el protocolo cifrado SSL.

- `-cert <path to certificate file>`: usa el archivo de certificado especificado para la autenticación del acceso al Servidor de administración.

  Si la clave no está en uso, el Agente de red recibe un certificado en la primera conexión al Servidor de administración.

- `-silent`: ejecutar la utilidad en modo silencioso.

  El uso de la clave puede ser útil, por ejemplo, si la utilidad se inicia desde el script de inicio de sesión al momento del registro del usuario.

- `-dupfix`: la clave se usa si el Agente de red se instaló mediante un método que difiere del usual (con el paquete de distribución); por ejemplo, si se recuperó a partir de una imagen de disco ISO.

- `-virtserv`: nombre del Servidor de administración virtual.

- `-cloningmode`: modo de clonación de disco del Agente de red.

  Use uno de los siguientes parámetros para configurar el modo de clonación de disco:

  - `-cloningmode`: solicitar el estado del modo de clonación de disco.
  - `-cloningmode 1`: habilitar el modo de clonación de disco.
  - `-cloningmode 0`: deshabilitar el modo de clonación de disco.

- `-nauninstpwd <password>`: la clave se utiliza para especificar la contraseña de desinstalación del Agente de red.

  La clave no es obligatoria.

Por ejemplo, para conectar el Agente de red al Servidor de administración, ejecute el siguiente comando:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

## Creación de un túnel de conexión entre un dispositivo cliente y el Servidor de administración

Kaspersky Security Center permite hacer túneles de conexión TCP desde la Consola de administración mediante el Servidor de administración y luego mediante el Agente de red a un puerto especificado en un dispositivo administrado. Gracias a este túnel, una aplicación cliente instalada en el mismo dispositivo que la Consola de administración puede conectarse a un puerto TCP de un dispositivo administrado incluso si no existe una vía de conexión directa entre la Consola de administración y ese dispositivo administrado.

Por ejemplo, los túneles se utilizan para establecer conexiones con un escritorio remoto, tanto para conectarse a una sesión existente, como para crear una sesión remota nueva.

También se pueden habilitar con herramientas externas. Por ejemplo, el administrador puede ejecutar la utilidad PuTTY, el cliente VNC y otras herramientas de esta manera.

La conexión entre el Servidor de administración y el dispositivo cliente remoto se debe hacer pasar por un túnel cuando el puerto que se utiliza para conectarse al Servidor de administración no está disponible en el dispositivo. El puerto del dispositivo podría no estar disponible en estos casos:

- el dispositivo remoto está conectado a una red local en la que se utiliza el mecanismo NAT;
- el dispositivo remoto está en la misma red local que el Servidor de administración, pero el puerto se ha cerrado con un firewall.

*Para crear un túnel de conexión entre un dispositivo cliente y el Servidor de administración:*

1. En el árbol de consola, seleccione la carpeta del grupo que incluye el dispositivo cliente.
2. En la pestaña **Dispositivos**, seleccione el dispositivo.
3. En el menú contextual del dispositivo, seleccione **Todas las tareas** → **Túnel de conexión**.
4. En la ventana **Túnel de conexión** que se abre, cree un túnel.

# Conexión remota al escritorio de un dispositivo cliente

El administrador puede obtener acceso remoto al escritorio de un dispositivo cliente a través de un Agente de red instalado en el dispositivo cliente.

El Agente de red permite conectarse incluso si el dispositivo cliente tiene cerrados los puertos TCP y UDP. Al establecer la conexión con el dispositivo, el administrador obtiene acceso completo a la información almacenada en este dispositivo, de manera que puede administrar las aplicaciones instaladas en él.

En esta sección se describe cómo establecer una conexión con un dispositivo cliente de Windows y un dispositivo cliente macOS a través del Agente de red.

## Conexión a dispositivos cliente de Windows

La conexión remota con un dispositivo se puede establecer de una de estas formas:

- Uso de un componente estándar de Microsoft Windows denominado Conexión a Escritorio remoto.

  La conexión con el escritorio remoto se establece a través de mstsc.exe, una utilidad que viene incluida en Windows, conforme a los ajustes de la utilidad.

- Mediante el uso de la tecnología de Windows Desktop Sharing.

## Conexión al dispositivo cliente de Windows usando la Conexión a Escritorio remoto

Si se conecta a la sesión de escritorio remoto establecida por un usuario, lo hará sin que el usuario lo sepa. Una vez que el administrador se conecta a la sesión, el usuario del dispositivo queda desconectado de la sesión sin notificación previa.

*Para conectarse al escritorio de un dispositivo cliente a través del componente de Conexión con el escritorio remoto:*

1. En el árbol de Consola de administración, seleccione el dispositivo al que debe obtener acceso.

2. En el menú contextual del dispositivo, seleccione **Todas las tareas → Conectarse al dispositivo → Nueva sesión de RDP**.

   Como resultado, se inicia la utilidad estándar de Windows mstsc.exe, que ayuda a establecer la conexión con el escritorio remoto.

3. Siga las instrucciones que se muestran en los cuadros de diálogo de la utilidad.

Una vez que se establezca la conexión con el dispositivo, tendrá acceso al escritorio a través de la ventana Conexión a Escritorio remoto de Microsoft Windows.

## Para conectarse al escritorio de un dispositivo cliente a través de Windows Desktop Sharing:

Al conectarse con una sesión existente del escritorio remoto, el usuario de la sesión en el dispositivo recibe una solicitud de conexión del administrador. No hay información acerca de la actividad remota del dispositivo, y los resultados se guardarán en informes creados por Kaspersky Security Center.

El administrador se puede conectar a una sesión existente en un dispositivo cliente sin desconectar al usuario de esta sesión. En tal caso, el acceso al escritorio se comparte entre el administrador y el usuario que inició la sesión.

El administrador puede configurar una auditoría de la actividad del usuario en un dispositivo cliente remoto. Durante la auditoría, la aplicación guarda información sobre los archivos del dispositivo cliente que el administrador haya abierto o modificado.

Para que pueda conectarse al escritorio de un dispositivo cliente a través de Windows Desktop Sharing, se deben cumplir las siguientes condiciones:

- La estación de trabajo del administrador debe tener Microsoft Windows Vista o una versión de Windows posterior. El tipo de sistema operativo del dispositivo que alberga al Servidor de administración no impone restricciones con respecto a la conexión a través de Windows Desktop Sharing.

  Para determinar si la característica Windows Desktop Sharing está disponible en su edición de Windows, verifique que la clave CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} esté presente en el registro de Windows.

- El dispositivo cliente debe tener Microsoft Windows Vista o una versión de Windows posterior.

- Kaspersky Security Center usa una licencia para la Administración de vulnerabilidades y parches.

*Para conectarse al escritorio de un dispositivo cliente a través de Escritorio compartido de Windows:*

1. En el árbol de Consola de administración, seleccione el dispositivo al que debe obtener acceso.

2. En el menú contextual del dispositivo, seleccione **Todas las tareas** → **Conectarse al dispositivo** → **Windows Desktop Sharing**.

3. En la ventana **Seleccionar sesión de escritorio remoto** que se abre, seleccione la sesión en el dispositivo a la que debe conectarse.

   Si la conexión al dispositivo se establece correctamente, el escritorio del dispositivo estará disponible en la ventana **Visor de sesiones del escritorio remoto de Kaspersky**.

4. Para comenzar a interactuar con el dispositivo, en el menú principal de la ventana **Visor de sesiones del escritorio remoto de Kaspersky**, seleccione **Acciones** → **Modo interactivo**.

Para la utilidad **Visor de sesiones del escritorio remoto de Kaspersky**, se necesita una licencia comercial.

## Conexión a dispositivos cliente macOS

El administrador puede usar el sistema de computación virtual en red (VNC) para conectarse a dispositivos macOS.

La conexión a un escritorio remoto se establece a través de un cliente VNC instalado en el dispositivo del Servidor de administración. El cliente VNC cambia el control del teclado y el ratón del dispositivo cliente al administrador.

Cuando el administrador se conecta al escritorio remoto, el usuario no recibe notificaciones ni solicitudes de conexión del administrador. El administrador se puede conectar a una sesión existente en un dispositivo cliente sin desconectar al usuario de esta sesión.

Para que pueda conectarse al escritorio de un dispositivo cliente a través de Windows Desktop Sharing, se deben cumplir las siguientes condiciones:

- El cliente VNC está instalado en el dispositivo del Servidor de administración.
- En el dispositivo cliente se permiten el inicio de sesión remoto y la administración remota.
- El usuario ha permitido que el administrador acceda al dispositivo cliente en la configuración de **Uso compartido** del sistema operativo macOS.

*Para conectarse al escritorio de un dispositivo cliente a través del componente de Conexión con el escritorio remoto:*

1. En el árbol de Consola de administración, seleccione el dispositivo al que debe obtener acceso.
2. En el menú contextual del dispositivo, seleccione **Todas las tareas** → **Túnel de conexión**.
3. En la ventana **Túnel de conexión** que se abre, realice una de las siguientes acciones:
   a. En la sección **1. Puerto de red**, especifique el número del puerto de red del dispositivo al que tiene que conectarse.
      De manera predeterminada, se utiliza el puerto 5900.
   b. En la sección **2. Túnel**, haga clic en el botón **Crear túnel**.
   c. En la sección **3. Configuración de red**, haga clic en el botón **Copiar**.
4. Abra el cliente VNC y pegue los atributos de red copiados en el campo de texto. Pulse **`Intro`**.
5. En la ventana que se abre, vea los detalles del certificado. Si acepta usar el certificado, haga clic en el botón **Sí**.
6. En la ventana **Autenticación**, especifique las credenciales del dispositivo cliente y, a continuación, haga clic en **Aceptar**.

## Conectarse a un dispositivo a través de Windows Desktop Sharing

*Para conectarse a un dispositivo mediante Windows Desktop Sharing:*

1. En el árbol de la consola, en la pestaña **Dispositivos**, seleccione la carpeta **Dispositivos administrados**.
   El espacio de trabajo de esta carpeta muestra una lista de dispositivos.
2. En el menú contextual del dispositivo al que desea conectarse, seleccione **Conectarse al dispositivo** → **Windows Desktop Sharing**.
   Se abre la ventana **Seleccionar sesión de escritorio remoto**.
3. En la ventana **Seleccionar sesión de escritorio remoto** seleccione una sesión de escritorio para conexión al dispositivo.
4. Haga clic en **Aceptar**.

El dispositivo está conectado.

## Configurar el reinicio de un dispositivo cliente

Al usar, instalar o eliminar Kaspersky Security Center, debería reiniciar el dispositivo. Solo se puede especificar la configuración de reinicio para dispositivos que funcionan con Windows.

*Para configurar el reinicio de un dispositivo cliente:*

1. En el árbol de consola, seleccione el grupo de administración para el que desea configurar el reinicio.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.
3. En el espacio de trabajo, seleccione una directiva del Agente de red de Kaspersky Security Center en la lista de directivas y luego seleccione **Propiedades** en el menú contextual de la directiva.
4. En la ventana de propiedades de la directiva, seleccione la sección **Opciones de reinicio**.
5. Seleccione la acción que se debe realizar si se requiere un reinicio del dispositivo:
   - Seleccione **No reiniciar el sistema operativo** para bloquear el reinicio automático.
   - Seleccione **Reiniciar el sistema operativo automáticamente si es necesario** para permitir el reinicio automático.
   - Seleccione **Solicitar al usuario una acción** para habilitar la solicitud al usuario para permitir el reinicio.

   Al seleccionar las casillas y la configuración de hora correspondientes en los selectores numéricos, puede especificar la frecuencia de las solicitudes de reinicio y habilitar el reinicio y cierre forzados de aplicaciones durante sesiones bloqueadas en el dispositivo.
6. Haga clic en **Aceptar** para guardar los cambios y cierre la ventana Propiedades de la directiva.

Ahora se configurará el reinicio del dispositivo.

## Auditoría de acciones en un dispositivo cliente remoto

La aplicación permite que se realice la auditoría de las acciones del administrador en un dispositivo cliente remoto que funcionan con Windows. Durante la auditoría, la aplicación guarda en el dispositivo información sobre los archivos que el administrador ha abierto o modificado. La auditoría de las acciones del administrador está disponible cuando se cumplen las siguientes condiciones:

- La licencia de Administración de vulnerabilidades y parches está en uso.
- El administrador tiene permiso para ejecutar el acceso compartido al escritorio del dispositivo remoto.

*Para habilitar la auditoría de acciones en un dispositivo cliente remoto:*

1. En el árbol de consola, seleccione el grupo de administración para el que se debe configurar la auditoría de las acciones del administrador.
2. En el espacio de trabajo del grupo, seleccione la pestaña **Directivas**.

3. Seleccione una directiva del Agente de red de Kaspersky Security Center y luego seleccione **Propiedades** en el menú contextual de la directiva.

4. En la ventana de propiedades de la directiva, seleccione la sección **Windows Desktop Sharing**.

5. Seleccione la casilla **Habilitar auditoría**.

6. En las listas **Máscaras de archivos cuya lectura debe monitorizarse** y **Máscaras de archivos cuya modificación debe monitorizarse**, agregue máscaras de archivos en las que la aplicación debe monitorear las acciones durante la auditoría.

   De forma predeterminada, la aplicación monitorea las acciones en los archivos con extensiones txt, rtf, doc, xls, docx, xlsx, odt y pdf.

7. Haga clic en **Aceptar** para guardar los cambios y cierre la ventana Propiedades de la directiva.

De esta manera, se configura la auditoría de las acciones del administrador en el dispositivo remoto del usuario con acceso compartido al escritorio.

Los registros de las acciones del administrador en el dispositivo remoto se computan:

- En el registro de eventos del dispositivo remoto.
- En un archivo con la extensión syslog ubicado en la carpeta del Agente de red de un dispositivo remoto (p. ej., C:\ProgramData\KasperskyLab\adminkit\1103\logs).
- En la base de datos de eventos de Kaspersky Security Center.

# Comprobación de la conexión entre un dispositivo cliente y el Servidor de administración

Kaspersky Security Center permite comprobar automática o manualmente las conexiones entre un dispositivo cliente y el Servidor de administración.

La comprobación automática de la conexión se ejecuta en el Servidor de administración. La comprobación manual de la conexión se ejecuta en el dispositivo.

## Comprobación automática de la conexión entre un dispositivo cliente y el Servidor de administración

*Para iniciar una comprobación automática de la conexión entre un dispositivo cliente y el Servidor de administración:*

1. En el árbol de consola seleccione el grupo de administración que incluye el dispositivo.

2. En el espacio de trabajo del grupo de administración, en la pestaña **Dispositivos** seleccione el dispositivo.

3. En el menú contextual del dispositivo, seleccione **Comprobar acceso al dispositivo**.

Se abre una ventana se abre que contiene la información sobre la accesibilidad del dispositivo.

## Comprobación manual de la conexión entre un dispositivo cliente y el Servidor de administración. Utilidad klnagchk

Puede comprobar la conexión y obtener información detallada sobre la configuración de la conexión entre un dispositivo cliente y el Servidor de administración mediante la utilidad klnagchk. La utilidad klnagchk se encuentra en la carpeta de instalación del Agente de red.

Al iniciarse desde la línea de comandos, la utilidad klnagchk puede realizar las siguientes acciones (dependiendo de las claves en uso):

- Se muestra en la pantalla o registra los valores de la configuración usada para conectar el Agente de red instalado en el dispositivo con el Servidor de administración.
- Registra en un archivo de registro del evento las estadísticas del Agente de red (desde el último inicio) y los resultados de la operación de la utilidad, o bien muestra la información en pantalla.
- Intenta establecer conexión entre el Agente de red y el Servidor de administración.

  Si falla el intento de conexión, la utilidad envía un paquete ICMP para comprobar el estado del dispositivo donde está instalado el Servidor de administración.

*Para comprobar la conexión entre un dispositivo cliente y el Servidor de administración mediante la utilidad klnagchk:*

En el dispositivo con el Agente de red instalado, inicie la utilidad klnagchk desde la línea de comandos con una cuenta de administrador local.

Sintaxis de línea de comandos de la utilidad:

```
klnagchk [-logfile <nombre del archivo>] [-sp] [-savecert <ruta al archivo del certificado>] [-restart][-sendhb]
```

Descripciones de las claves:

- `-logfile <nombre del archivo>`: registra en un archivo de registro los valores de la configuración de conexión entre el Agente de red y el Servidor de administración y los resultados de la operación de la utilidad.

  De manera predeterminada, la información se guarda en el flujo saliente estándar (stdout). Si la clave no está en uso, la configuración, los resultados y mensajes de error se muestran en pantalla.
- `-sp`: muestra la contraseña para la autenticación del usuario en el servidor proxy.

  La clave está en uso si la conexión al Servidor de administración se establece a través de un servidor proxy.
- `-savecert <nombre del archivo>`: guarda el certificado utilizado para acceder al Servidor de administración, en un archivo especificado.
- `-restart`: inicia el Agente de red una vez completada la utilidad.
- `-sendhb`: inicia la sincronización del Agente de red con el Servidor de administración.

Después del inicio, la utilidad klnagchk accede a los archivos de configuración del Agente de red y muestra los parámetros de conexión. Estos parámetros se especifican durante la instalación del Agente de red y en la configuración de la directiva del Agente de red:

- `Current device`: nombre de red de Windows del dispositivo cliente.
- `Network Agent version`: número completo de la versión del Agente de red (con parches) instalada en el dispositivo.
- `Administration Server address`: dirección del Servidor de administración.
- `Use SSL`: parámetro que indica si se utiliza una conexión segura al conectarse al Servidor de administración.

  Valores posibles:

  - 0: no se utiliza una conexión segura.
  - 1: se utiliza una conexión segura.
- `Compress traffic`: parámetro que indica si el tráfico entre el dispositivo cliente y el Servidor de administración está comprimido.
- `Numbers of the Administration Server SSL ports`: número de puertos válidos para la comunicación con el Servidor de administración cuando se utiliza una conexión segura.
- `Numbers of the Administration Server ports`: número de puertos válidos para la comunicación con el Servidor de Administración cuando se utiliza una conexión ordinaria.
- `Use proxy server`: parámetro que indica si se utiliza un servidor proxy.

  Valores posibles:

  - 0: no se utiliza un servidor proxy.
  - 1: se utiliza un servidor proxy.
- `Address`: dirección y puerto del servidor proxy, separados por dos puntos. Este parámetro se muestra solo si se utiliza un servidor proxy.
- `User name`: nombre de usuario para acceder al servidor proxy. Este parámetro se muestra solo si se utiliza un servidor proxy.
- `Password`: contraseña para acceder al servidor proxy. Este parámetro se muestra solo si se utiliza un servidor proxy. Para mostrar la contraseña del servidor proxy, debe usar la clave `sp` en el comando.
- `Administration Server certificate`: parámetro que indica si el dispositivo cliente tiene un certificado del Servidor de administración. Es posible que no exista un certificado, por ejemplo, si el Agente de red nunca se conectó correctamente al Servidor de administración.

  Valores posibles:

  - `not installed`: el dispositivo cliente no tiene un certificado de servidor de administración.
  - `available`: el dispositivo cliente tiene un certificado de servidor de administración.

- `Open UDP port`: parámetro que indica si el Agente de red usa el puerto UDP para recibir solicitudes de sincronización del Servidor de administración.

  Valores posibles:

  - 0: el puerto UDP está cerrado para recibir solicitudes de sincronización del Servidor de administración.
  - 1: el puerto UDP está abierto para recibir solicitudes de sincronización del Servidor de administración.

- `Numbers of UDP ports`: números de los puertos UDP que puede utilizar el Agente de red.
- `Location name`: ubicación de red del dispositivo.
- `State of network location`: parámetro que indica si el dispositivo cliente se puede cambiar de un perfil de conexión del Servidor de administración a otro.

  Valores posibles:

  - `Enabled`: el perfil de conexión del servidor de administración se puede cambiar para el dispositivo cliente.
  - `Disabled`: el perfil de conexión del Servidor de administración no se puede cambiar para el dispositivo cliente.

- `Profile to use`: perfil de conexión para el Servidor de administración.
- `Condition`: dirección IP y máscara de subred de la red a la que está conectado el dispositivo cliente.
- `Synchronization interval (min)`: intervalo estándar entre sincronizaciones.
- `Connection timeout (in seconds)`: tiempo de espera de conexión.
- `Send / receive timeout (in seconds)`: tiempo de espera de conexión en operaciones de lectura y escritura.
- `Device ID`: identificador del dispositivo en la red. El `Device ID` es único entre los dispositivos cliente administrados por un Servidor de administración en particular.
- `Locations of connection gateways`: parámetros para conectar el dispositivo cliente al Servidor de administración a través de la puerta de enlace de conexión.
- `Location of distribution points`: parámetros para conectar el dispositivo cliente al Servidor de administración a través del punto de distribución.

- `Connection with server`: parámetro que indica si la puerta de enlace de conexión tiene una conexión continua al Servidor de administración. El parámetro solo se muestra si el dispositivo cliente actúa como puerta de enlace de conexión.

  Valores posibles:

  - `active`: la pasarela de conexión tiene una conexión continua al Servidor de administración.
  - `inactive`: la pasarela de conexión no tiene una conexión continua al Servidor de administración.

- `Connection with server through connection gateway`: parámetro que indica si la conexión al Servidor de Administración a través de una pasarela de conexión se establece correctamente. El parámetro solo se muestra si el dispositivo cliente actúa como puerta de enlace de conexión.

  Valores posibles:

  - `active`: la conexión al Servidor de administración a través de una pasarela de conexión se estableció correctamente.
  - `inactive`: la conexión al Servidor de administración a través de una pasarela de conexión se estableció incorrectamente.

Además, el resultado de la utilidad klnagchk puede contener una de las siguientes líneas:

- `Administration Server is installed on this device`: la utilidad klnagchk se ejecuta en el dispositivo del Servidor de administración.
- `This device has been assigned a connection gateway but is not yet registered on Administration Server`: la utilidad klnagchk se ejecuta en el dispositivo en el que está instalado el Agente de red, en el modo de puerta de enlace de conexión. La puerta de enlace de conexión configurada está esperando una conexión del Servidor de administración, pero el Servidor de administración no enumera el dispositivo entre los dispositivos administrados. Debe asegurarse de que el Servidor de administración inicia una conexión a la puerta de enlace de conexión.
- `This device is a connection gateway`: la utilidad klnagchk se ejecuta en el dispositivo que actúa como pasarela de conexión.
- `Acts as a distribution point`: la utilidad klnagchk se ejecuta en el dispositivo que actúa como punto de distribución.

La utilidad klnagchk comprueba el estado del servicio del Agente de red. Si el servicio no se está ejecutando, la utilidad se detiene. Si el servicio se está ejecutando, la utilidad muestra las siguientes estadísticas de conexión:

- `Total number of synchronization requests`: número de intentos para conectar el dispositivo cliente al Servidor de administración.
- `The number of successful synchronization request`: número de intentos exitosos para conectar el dispositivo cliente al Servidor de administración.
- `Total number of synchronizations`: número de intentos para sincronizar la configuración del dispositivo cliente con la configuración del Servidor de administración.
- `The number of successful synchronizations`: número de intentos exitosos para sincronizar la configuración del dispositivo cliente con el Servidor de administración.
- `Date/time of the last request for synchronization`: fecha y hora de la última conexión.

Debe utilizar los parámetros `Total number of synchronization requests` y `The number of successful synchronization request` cuando analiza la conexión entre el Servidor de administración y el Agente de red. La configuración del dispositivo cliente se sincroniza con la configuración del Servidor de administración solo si se modificó la configuración del Servidor de administración (por ejemplo, si se agregaron nuevas tareas o se modificó la configuración de la directiva). De lo contrario, los valores de los parámetros `Total number of synchronizations` y `The number of successful synchronizations` permanecen sin cambios.

Para obtener más información sobre cómo solucionar problemas relacionados con la conexión del Agente de red al Servidor de administración, consulte las Preguntas frecuentes de Kaspersky Security Center.

### Acerca de la comprobación de la hora de conexión entre un dispositivo y el Servidor de administración

Cuando se apaga un dispositivo, el Agente de red notifica el Servidor de administración de este evento. En la Consola de administración, ese dispositivo se muestra como apagado. Sin embargo, el Agente de red no puede notificar el Servidor de administración de todos los eventos de este tipo. El Servidor de administración, por lo tanto, periódicamente analiza el atributo **Conectado al Servidor de administración** (el valor de este atributo se muestra en la Consola de administración, en las propiedades del dispositivo, en la sección **General**) para cada dispositivo y lo compara con el intervalo de sincronización de la configuración actual del Agente de red. Si un dispositivo no ha respondido durante más de tres intervalos de sincronización sucesivos, ese dispositivo se marca como apagado.

## Identificación de dispositivos cliente en el Servidor de administración

Los dispositivos cliente se identifican según sus nombres. El nombre de un dispositivo es único entre todos los nombres de los dispositivos conectados al Servidor de administración.

El nombre de un dispositivo se transfiere al Servidor de administración cuando se sondea la red de Windows y se detecta un nuevo dispositivo, o bien durante la primera conexión del Agente de red instalado en un dispositivo al Servidor de administración. De manera predeterminada, el nombre coincide con el nombre del dispositivo en la red de Windows (nombre NetBIOS). Si un dispositivo con este nombre ya está registrado en el Servidor de administración, se agregará un índice con el siguiente número de secuencia al nombre del nuevo dispositivo, por ejemplo: **<Nombre>-1**, **<Nombre>-2**. Bajo este nombre, el dispositivo se agrega al grupo de administración.

## Mover dispositivos a un grupo de administración

Puede mover dispositivos de un grupo de administración a otro solo si tiene el permiso **Modificar** en el área **Administración de grupos de administración** para los grupos de administración de origen y destino (o para el Servidor de administración al que pertenecen estos grupos).

*Para incluir uno o varios dispositivos en un grupo de administración seleccionado:*

1. En el árbol de consola, expanda la carpeta **Dispositivos administrados**.
2. En la carpeta **Dispositivos administrados**, seleccione la subcarpeta que corresponde al grupo en el cual se incluirán los dispositivos cliente.

   Si desea incluir los dispositivos en el grupo **Dispositivos administrados**, puede omitir este paso.
3. En el espacio de trabajo del grupo de administración seleccionado, en la pestaña **Dispositivos**, inicie el proceso de inclusión de dispositivos en el grupo mediante uno de los siguientes métodos:

   - Al agregar los dispositivos al grupo, haga clic en el botón **Mover dispositivos al grupo** en el cuadro de información de la lista de dispositivos
   - Seleccione **Crear → Dispositivo** en el menú contextual de la lista de dispositivos

   Se inicia el Asistente para mover dispositivos. Siguiendo sus instrucciones, seleccione un método para mover los dispositivos al grupo y crear una lista de dispositivos que se incluirán en el grupo.

   Si crea una lista de dispositivos en forma manual, puede utilizar una dirección IP (o un intervalo IP), un nombre NetBIOS o un nombre DNS como dirección del dispositivo. Solo puede mover manualmente a la lista dispositivos para los cuales ya se agregó información a la base de datos del Servidor de administración cuando se conectó el dispositivo o luego del descubrimiento de dispositivos.

   Para importar una lista de dispositivos desde un archivo, especifique un archivo TXT con una lista de direcciones de los dispositivos que se agregarán. Cada dirección debe ser especificada en una línea separada.

Una vez finalizado el asistente, los dispositivos seleccionados se incluyen en el grupo de administración y se muestran en la lista de dispositivos con nombres generados por el Servidor de administración.

Puede mover un dispositivo al grupo de administración seleccionado arrastrándolo desde la carpeta de dispositivos **Dispositivos no asignados** a la carpeta de ese grupo de administración.

## Cambiar los dispositivos cliente de Servidor de administración

Puede cambiar el Servidor de administración que administra los dispositivos cliente por otro, mediante la tarea *Cambiar Servidor de administración*.

*Para cambiar el Servidor de administración que administra ciertos dispositivos cliente:*

1. En el árbol de la consola, seleccione la carpeta **Tareas**.
2. En el espacio de trabajo de esta carpeta, haga clic en el botón **Nueva tarea**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
3. En el paso **Seleccione el tipo de tarea** del asistente, seleccione el nodo **Kaspersky Security Center Administration Server**, expanda la carpeta **Avanzado**, y luego seleccione la tarea **Cambiar Servidor de administración**.

4. En la ventana que se abre, haga clic en el botón **Aceptar** para confirmar que acepta los términos del cambio del Servidor de administración para los dispositivos cliente.

5. En el paso **Configuración** del asistente, seleccione el Servidor de administración que desea utilizar para administrar los dispositivos seleccionados:

   - Cambiar a otro Servidor de administración principal

     Para mover dispositivos cliente a otro servidor de administración principal, especifique los siguientes ajustes de conexión del servidor de administración:

     1. En el campo **Servidor de administración** especifique la dirección del nuevo servidor de administración principal.
     2. En el campo **Puerto** especifique el número de puerto para conectarse al Servidor de administración.

        El número de puerto predeterminado es 14000.
     3. En el campo **Puerto SSL** especifique el número del puerto SSL en el Servidor de administración principal.

        El número de puerto predeterminado es 13000.
     4. Seleccione la casilla de verificación **Usar servidor proxy**.

        Si esta opción no está marcada, se utiliza la conexión directa para conectar el dispositivo al Servidor de administración.

        Si esta opción está marcada, especifique los parámetros del servidor proxy:

        - **Dirección del servidor proxy**
        - **Puerto del servidor proxy**

        Si su servidor proxy requiere autenticación, en los campos **Nombre de usuario** y **Contraseña**, indique las credenciales de la cuenta con la que se establece la conexión con el servidor proxy. Le recomendamos que utilice las credenciales de una cuenta que solamente tenga los privilegios mínimos necesarios para completar la autenticación ante el servidor proxy.
     5. Si es necesario, cargue un nuevo certificado del Servidor de Administración.

   - Cambiar a otro Servidor virtual de este Servidor principal

     Seleccione esta opción para mover los dispositivos cliente al Servidor de administración virtual en el Servidor de administración principal actual. Para ello, en el campo **Nombre del Servidor de administración virtual** especifique el nombre del Servidor de administración virtual necesario.

   Si es necesario, especifique el tiempo de espera antes de reiniciar el Agente de red.

6. En este paso del asistente, seleccione los dispositivos a los que se asignará la tarea:

   - **Seleccionar dispositivos de la red detectados por el Servidor de administración**. En este caso, la tarea se asigna a dispositivos específicos. Estos pueden ser tanto dispositivos asignados a grupos de administración como dispositivos no asignados.

   - **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**. Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

   - **Asignar tarea a una selección de dispositivos**. En este caso, la tarea se asigna a los dispositivos incluidos en una selección creada anteriormente. Puede especificar la selección predeterminada o una personalizada que haya creado.

   - **Asignar tarea a un grupo de administración**. En este caso, la tarea se asigna a los dispositivos incluidos en el grupo de administración creado anteriormente.

7. En el paso **Seleccione una cuenta para ejecutar la tarea** del asistente, especifique la configuración de la cuenta:

   - Cuenta predeterminada

     La tarea se ejecutará utilizando la misma cuenta que la aplicación que realizará la tarea.

     Esta opción está seleccionada de forma predeterminada.

   - Especificar cuenta

     Complete los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta con la que se ejecutará la tarea. La cuenta debe tener los derechos necesarios para realizar la tarea.

     - Cuenta

       Cuenta con la que se ejecutará la tarea.

     - Contraseña

       Contraseña de la cuenta con la que se ejecutará la tarea.

8. En la página **Configurar programación de tarea**, puede crear una programación para el inicio de la tarea. De ser necesario, configure los siguientes ajustes:

- Inicio programado:

  Seleccione y configure la programación según la cual se ejecutará la tarea.

  - Diario (no compatible con horario de verano)

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta programación no tiene en cuenta los cambios de horario estacionales. La hora de inicio de la tarea se mantendrá sin cambios incluso si el reloj se atrasa o se adelanta una hora debido al horario de verano.

    No recomendamos usar esta programación. Se la ofrece para mantener la compatibilidad con versiones anteriores de Kaspersky Security Center.

    De forma predeterminada, la tarea se iniciará todos los días a la hora actual del sistema.

  - Por días de la semana

    La tarea se ejecutará periódicamente en los días de la semana y a la hora que indique.

    De manera predeterminada, la tarea se ejecutará todos los viernes a las 18:00:00.

  - Mensual

    La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

    Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

    Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

  - Una vez

    La tarea se ejecuta una vez, en la fecha y hora especificadas (de manera predeterminada, el día en que se creó la tarea).

  - Manual

    La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

    Esta opción está seleccionada de forma predeterminada.

  - Inmediatamente

    La tarea se ejecuta inmediatamente después de que el dispositivo se hace visible en la red o inmediatamente después de que el dispositivo se incluye en el alcance de la tarea.

- Ejecutar tareas no realizadas

Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

Esta opción está deshabilitada de forma predeterminada.

- **Esperar un tiempo definido al azar antes de iniciar la tarea**

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

- **Limitar el tiempo de espera a esta cantidad de minutos**

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

  Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

9. En este paso del asistente, especifique el nombre de la tarea que está creando.

10. En el paso **Finalizar la creación de la tarea** del asistente, haga clic en el botón **Finalizar** para cerrar el asistente.

    Para que la tarea se inicie en cuanto se cierre el asistente, marque la casilla **Ejecutar la tarea al finalizar el asistente**.

Una vez que se completa la tarea, los dispositivos cliente para los que se la creó quedan bajo el mando del Servidor de administración especificado en la configuración de la tarea.

Si el Servidor de administración admite el cifrado y la protección de datos y usted está creando una tarea *Cambiar Servidor de administración*, se mostrará una advertencia. La advertencia estipula que, si algunos datos cifrados se almacenan en dispositivos, después de que el Servidor nuevo comience a administrar los dispositivos, los usuarios podrán acceder solo a los datos cifrados con los cuales trabajaron anteriormente. En otros casos, no se brindará acceso a datos cifrados. Para más precisiones sobre los casos en los que se pierde el acceso a la información cifrada, consulte la Ayuda de Kaspersky Endpoint Security para Windows.

## Mover dispositivos conectados a un Servidor de administración mediante puertas de enlace de conexión a otro Servidor de administración

Puede mover los dispositivos conectados a un Servidor de administración mediante puertas de enlace de conexión a otro Servidor de administración. Esto puede ser necesario si, por ejemplo, instala otra versión del Servidor de administración y no desea reinstalar el Agente de red en los dispositivos, ya que ello puede llevar mucho tiempo.

Los comandos descritos en las instrucciones deben ejecutarse en los dispositivos cliente utilizando una cuenta con derechos de administrador.

*Para mover un dispositivo conectado mediante una puerta de enlace de conexión a otro Servidor de administración:*

1. Ejecute la utilidad klmover con el parámetro `-address <dirección del servidor>`, para cambiar al nuevo Servidor de Administración.
2. Ejecute el comando `klnagchk -nagwait -tl 4`.
3. Ejecute los siguientes comandos para establecer una nueva puerta de enlace de conexión:
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "<ip_o_nombre_de_puerta_de_enlace>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     Aquí `gateway_ip_or_name` es la dirección de la puerta de enlace de conexión a la que se puede acceder desde Internet.
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

     `13000` es el número del puerto TCP en el que recibe solicitudes la puerta de enlace de conexión
4. Ejecute el comando `klnagchk -restart -tl 4` para iniciar el servicio del Agente de red.

El dispositivo se mueve al nuevo Servidor de administración y se conecta a través de la nueva puerta de enlace conectada.

## Clústeres y conjuntos de servidores

Kaspersky Security Center admite la tecnología de clúster. Si el Agente de red envía información al Servidor de administración que confirma que la aplicación instalada en un dispositivo cliente forma parte de una matriz de servidores, el dispositivo cliente se convierte en un nodo del clúster. El clúster se agregará como objeto individual en la carpeta **Dispositivos administrados** del árbol de consola con el icono de servidores ( ).

Se pueden distinguir algunas funciones comunes de un clúster:

- Un clúster y cualquiera de sus nodos siempre están en el mismo grupo de administración.
- Si el administrador intenta mover un nodo del clúster, el nodo regresa a su ubicación original.
- Si el administrador intenta mover un clúster a un grupo diferente, todos sus nodos también se moverán con él.

## Encendido, apagado y reinicio remoto de dispositivos cliente

Kaspersky Security Center permite que usted administre dispositivos cliente remotamente al activarlos, apagarlos o reiniciarlos.

*Para administrar remotamente dispositivos cliente:*

1. Conéctese al Servidor de administración que administra los dispositivos.
2. Cree una tarea de administración de dispositivos mediante uno de los métodos siguientes:
   - Si necesita encender, apagar o reiniciar dispositivos incluidos en el grupo de administración seleccionado, cree una tarea de grupo para el grupo seleccionado.
   - Si necesita encender, apagar o reiniciar dispositivos incluidos en distintos grupos de administración o que no pertenecen a ninguno, cree una tarea para dispositivos específicos.

   Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente. En la ventana **Seleccione el tipo de tarea** del Asistente para crear nueva tarea, seleccione el nodo **Kaspersky Security Center**, abra la carpeta **Avanzado** y seleccione la tarea **Administrar dispositivos**.
3. Ejecute la tarea creada.

   Luego de finalizar la tarea, se ejecutará el comando (encender, apagar o reiniciar) en los dispositivos seleccionados.

# Acerca del uso de la conexión continua entre un dispositivo administrado y el Servidor de administración

De forma predeterminada, Kaspersky Security Center no presenta la conectividad continua entre dispositivos administrados y el Servidor de administración. Los Agentes de red en los dispositivos administrados periódicamente establecen conexiones y se sincronizan con el Servidor de administración. El intervalo entre esas sesiones de sincronización se define en una directiva del Agente de red y es de 15 minutos de forma predeterminada. Si se requiere una sincronización temprana (por ejemplo, para forzar la aplicación de una directiva), el Servidor de administración envía un paquete de red firmado al Agente de red en el puerto UDP 15 000 (El Servidor de administración puede enviar este paquete a través de una red IPv4 o IPv6). Si, por algún motivo, no es posible establecer una conexión a través de UDP entre el Servidor de administración y un dispositivo administrado, la sincronización se ejecuta en la siguiente conexión rutinaria entre el Agente de red y el Servidor de administración dentro del intervalo de sincronización.

Sin embargo, algunas operaciones no pueden realizarse sin una conexión temprana entre el Agente de red y el Servidor de administración. Estas operaciones incluyen la ejecución y detención de tareas locales, la recepción de estadísticas de una aplicación administrada y la creación de un túnel. Para posibilitar estas operaciones, debe habilitar la opción **No desconectar del Servidor de administración** en el dispositivo administrado.

# Acerca de la sincronización forzada

Aunque Kaspersky Security Center automáticamente sincroniza el estado, la configuración, las tareas y las directivas para dispositivos administrados, en algunos casos el administrador tiene que saber exactamente si la sincronización se ha realizado ya para un dispositivo especificado en este momento.

En el menú contextual de dispositivos administrados en la Consola de administración, el elemento de menú **Todas las tareas** contiene el comando **Forzar sincronización**. Cuando Kaspersky Security Center 15.1 ejecuta este comando, el Servidor de administración intenta conectarse con el dispositivo seleccionado. Si la conexión se establece, se realiza una sincronización forzada en ese momento. Si la comunicación no puede establecerse, la sincronización forzada se pospone hasta la siguiente conexión programada entre el Agente de red y el Servidor de administración.

# Sobre la programación de conexión

En la ventana de propiedades del Agente de red, en la sección **Conectividad**, en la subsección **Programación de conexiones**, puede especificar intervalos de tiempo durante los cuales el Agente de red transmitirá datos al Servidor de administración.

**Conectar cuando sea necesario**. Si se selecciona esta opción, la conexión se establece cuando el Agente de red debe enviar datos al Servidor de administración.

**Conectarse en intervalos de tiempo especificados**. Si se selecciona esta opción, el Agente de red se conecta al Servidor de administración a una hora especificada. Puede agregar varios períodos de conexión.

## Envío de mensajes a usuarios de dispositivos

*Para enviar un mensaje por correo electrónico a usuarios de dispositivos:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. Cree la tarea de envío de mensajes a usuarios de dispositivos de una de las siguientes formas:
   - Si desea enviar un mensaje a los usuarios de dispositivos que pertenecen al grupo de administración seleccionado, cree una tarea para el grupo seleccionado.
   - Si desea enviar un mensaje a los usuarios de dispositivos que pertenecen a diferentes grupos de administración o no pertenecen a ninguno, cree una tarea para dispositivos específicos.

   Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente.
3. En la ventana tipo de tarea del Asistente para crear nueva tarea, seleccione el nodo **Servidor de administración de Kaspersky Security Center**, abra la carpeta **Avanzado** y seleccione la tarea **Enviar mensaje a usuario**. La tarea de enviar mensajes al usuario solo está disponible para dispositivos que funcionan con Windows. También puede enviar mensajes en el menú contextual del usuario en la carpeta **Cuentas de usuario**.
4. Ejecute la tarea creada.

   Una vez finalizada la tarea, el mensaje creado se enviará a los usuarios de los dispositivos seleccionados. La tarea de enviar mensajes al usuario solo está disponible para dispositivos que funcionan con Windows. También puede enviar mensajes en el menú contextual del usuario en la carpeta **Cuentas de usuario**.

## Administración de Kaspersky Security for Virtualization

Kaspersky Security Center admite la opción de conexión de máquinas virtuales con el Servidor de administración. Las máquinas virtuales están protegidas por Kaspersky Security for Virtualization. Para más información, consulte la documentación de esta aplicación.

## Configurar cambios de estado para los dispositivos

Puede cambiar las condiciones bajo las cuales se le asignan los estados *Crítico* o *Advertencia* a un dispositivo.

*Para habilitar el cambio de estado a Crítico para los dispositivos:*

1. Abra la ventana Propiedades de una de las siguientes formas:
   - En la carpeta **Directivas**, en el menú contextual de una directiva del Servidor de administración, seleccione **Propiedades**.
   - Seleccione **Propiedades** en el menú contextual de un grupo de administración.
2. En la ventana **Propiedades** que se abre, en el panel **Secciones**, seleccione **Estado del dispositivo**.

3. En el panel derecho, en la sección **Fijar en Crítico si esto se cumple**, marque la casilla junto a una de las condiciones de la lista.

   Solo puede cambiar la configuración que no esté bloqueada en la directiva primaria.

4. Haga doble clic en el nombre de la condición seleccionada y, a continuación, en la ventana que se abre, establezca el valor requerido para la condición.

   No puede establecer valores para las siguientes condiciones: La aplicación de seguridad no está instalada, Hay aplicaciones incompatibles instaladas, Se detectaron vulnerabilidades de software, La configuración del dispositivo móvil no cumple con la directiva, Problemas de seguridad no procesados detectados, Estado del dispositivo definido por la aplicación, El dispositivo ha cambiado a no administrado, La aplicación de seguridad no está en ejecución, La licencia caducó.

   Para la condición **Se debe reiniciar el dispositivo**, puede especificar los motivos del reinicio. Le recomendamos que seleccione las casillas junto a todos los motivos de la lista.

5. Haga clic en **Aceptar**.

Cuando se cumplan las condiciones especificadas, se asignará el estado *Crítico* al dispositivo administrado.

*Para habilitar el cambio de estado a Advertencia para los dispositivos:*

1. Abra la ventana Propiedades de una de las siguientes formas:

   - En la carpeta **Directivas**, en el menú contextual de una directiva del Servidor de administración, seleccione **Propiedades**.
   - Seleccione **Propiedades** en el menú contextual del grupo de administración.

2. En la ventana **Propiedades** que se abre, en el panel **Secciones**, seleccione **Estado del dispositivo**.

3. En el panel derecho, en la sección **Fijar en Advertencia si esto se cumple**, marque la casilla junto a una de las condiciones de la lista.

   Solo puede cambiar la configuración que no esté bloqueada en la directiva primaria.

4. Haga doble clic en el nombre de la condición seleccionada y, a continuación, en la ventana que se abre, establezca el valor requerido para la condición.

   No puede establecer valores para las siguientes condiciones: La aplicación de seguridad no está instalada, Hay aplicaciones incompatibles instaladas, Se detectaron vulnerabilidades de software, La configuración del dispositivo móvil no cumple con la directiva, Problemas de seguridad no procesados detectados, Estado del dispositivo definido por la aplicación, El dispositivo ha cambiado a no administrado, La aplicación de seguridad no está en ejecución, La licencia caducó.

   Para la condición **Se debe reiniciar el dispositivo**, puede especificar los motivos del reinicio. Le recomendamos que seleccione las casillas junto a todos los motivos de la lista.

5. Haga clic en **Aceptar**.

Cuando se cumplan las condiciones especificadas, se asignará el estado *Advertencia* al dispositivo administrado.

# Etiquetado de dispositivos y visualización de etiquetas asignadas

Kaspersky Security Center le permite etiquetar dispositivos. Una *etiqueta* es el ID de un dispositivo que se puede utilizar para agrupación, descripción o búsqueda de dispositivos. Las etiquetas asignadas a dispositivos se pueden utilizar para crear selecciones, para encontrar dispositivos y para distribuir dispositivos entre grupos de administración.

Puede etiquetar dispositivos manual o automáticamente. Etiquete un dispositivo manualmente en las propiedades del dispositivo; puede usar el etiquetado manual cuando tiene que etiquetar un dispositivo particular. El autoetiquetado es realizado por el Servidor de administración de acuerdo con las reglas de etiquetado especificadas.

En las propiedades de un Servidor de administración, puede configurar el autoetiquetado para dispositivos administrados por este Servidor de administración. Los dispositivos se etiquetan automáticamente cuando reúnen las condiciones de las reglas configuradas. Cada regla está asociada a una sola etiqueta. Las reglas atienden a las propiedades de cada dispositivo, como sus atributos de red, su sistema operativo o las aplicaciones que tiene instaladas. Por ejemplo, puede configurar una regla que asignará la etiqueta *Win* a todos los dispositivos que ejecuten Windows. A continuación, puede usar esta etiqueta al crear una selección de dispositivos; esto lo ayudará a clasificar todos los dispositivos que ejecuten Windows y les asignan una tarea.

También puede usar etiquetas como condiciones de activación del perfil de directivas en un dispositivo administrado a fin de aplicar perfiles de directivas específicos solo en dispositivos con etiquetas específicas. Por ejemplo, si un dispositivo etiquetado como *Courier* aparece en el grupo de administración *Usuarios* y si la activación del perfil de directiva correspondiente mediante la etiqueta *Courier* se ha habilitado, entonces la directiva creada para el grupo *Usuarios* no se aplicará a este dispositivo, pero el perfil del perfil de directiva se aplicará. El perfil de directivas puede permitir que este dispositivo inicie algunas aplicaciones que se han bloqueado para no ser ejecutadas mediante la directiva.

Puede crear más de una regla de etiquetado. Si crea varias reglas de etiquetado y un dispositivo cumple simultáneamente con las condiciones de todas ellas, dicho dispositivo recibirá varias etiquetas. Puede ver la lista de todas las etiquetas asignadas en las propiedades del dispositivo. Cada regla de etiquetado se puede habilitar o deshabilitar. Si una regla se habilita, se aplica a dispositivos administrados por el Servidor de administración. Si no usa una regla actualmente, pero la puede necesitar en el futuro, no la tiene que eliminar; simplemente puede desactivar la casilla **Habilitar regla**. En este caso, la regla se deshabilita; no se ejecutará hasta que la casilla **Habilitar regla** se seleccione de nuevo. Es posible que tenga que deshabilitar una regla sin eliminarla si tiene que excluir la regla de la lista de reglas de etiquetado temporalmente y luego incluirla de nuevo.

## Etiquetado automático de dispositivos

Puede crear y modificar reglas de etiquetado automáticas en la ventana de propiedades Servidor de administración.

*Etiquetar dispositivos automáticamente:*

1. En el árbol de la consola, seleccione el nodo con el nombre del Servidor de administración para el cual tiene que especificar reglas de etiquetado.

2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.

3. En la ventana de propiedades del Servidor de administración, seleccione la sección **Reglas de etiquetado**.

4. En la sección **Reglas de etiquetado**, haga clic en el botón **Agregar**.

   Se abre la ventana **Nueva regla**.

5. En la ventana **Nueva regla**, configure las propiedades generales de la regla:

   - Especifique el nombre de la regla.

     El nombre de la regla no puede tener más de 255 caracteres ni incluir caracteres especiales (como `"*<>?\:|`).

   - Habilite o deshabilite la regla mediante la casilla **Habilitar regla**.

     La casilla de verificación **Habilitar regla** está seleccionada de manera predeterminada.

   - En el campo **Etiqueta**, escriba el nombre de la etiqueta.

     El nombre de la etiqueta no puede tener más de 255 caracteres y no puede incluir ningún carácter especial (como `"*<>?\:|`).

6. En la sección **Condiciones**, haga clic en el botón **Agregar** para agregar una condición nueva o haga clic en el botón **Propiedades** para editar una condición existente.

   Se abre la ventana del Asistente de nueva condición de regla de autoetiquetado.

7. En la ventana **Condición de asignación de etiquetas**, seleccione las casillas para las condiciones que deben afectar el etiquetado. Puede seleccionar varias condiciones.

8. Dependiendo de qué condiciones de etiquetado seleccionó, el Asistente muestra las ventanas para la instalación de las condiciones correspondientes. Configure la aplicación de la regla al darse las siguientes condiciones:

   - **Uso o asociación del dispositivo con una red específica**: Propiedades de la Red del dispositivo, por ejemplo nombre del dispositivo en la red Windows e inclusión del dispositivo en un dominio o una subred IP.

     > Si la intercalación con diferenciación entre mayúsculas y minúsculas está configurada para la base de datos utilizada para Kaspersky Security Center, respete las mayúsculas y minúsculas cuando ingrese el nombre DNS de un dispositivo. De lo contrario, la regla de etiquetado automático no funcionará.

   - **Uso de Active Directory**: presencia del dispositivo en una unidad organizativa o grupo de Active Directory.

   - **Aplicaciones específicas**: presencia del Agente de red en el dispositivo, tipo y versión de sistema operativo, arquitectura del sistema operativo.

   - **Máquinas virtuales**: Inclusión del dispositivo en un tipo concreto de máquinas virtuales.

   - **Presencia de una aplicación del registro de aplicaciones**: presencia de aplicaciones de distintos proveedores en el dispositivo.

9. Después de que la condición esté configurada, ingrese un nombre para ella y luego cierre el Asistente.

   Si es necesario, puede especificar varias condiciones para una misma regla. En ese caso, la etiqueta se asignará a cualquier dispositivo que cumpla con al menos una condición. Las condiciones que ha añadido se mostrarán en la ventana de propiedades de la regla.

10. Haga clic en **Aceptar** en la ventana **Nueva regla**, luego haga clic en **Aceptar** en la ventana de propiedades Servidor de administración.

Las reglas recién creadas se hacen cumplir en dispositivos administrados por el Servidor de administración seleccionado. Si la configuración de un dispositivo cumple con las condiciones de la regla, ese dispositivo recibirá la etiqueta.

### Visualización y configuración de etiquetas asignadas a un dispositivo

Puede ver la lista de todas las etiquetas que se han asignado a un dispositivo, así como van a la instalación de reglas de etiquetado automáticas en la ventana de propiedades del dispositivo.

*Ver y configurar las etiquetas que se han asignado a un dispositivo:*

1. Abra la carpeta **Dispositivos administrados** en el árbol de consola.
2. En el espacio de trabajo de la carpeta **Dispositivos administrados**, seleccione el dispositivo para el cual desea ver las etiquetas asignadas.
3. En el menú contextual del dispositivo móvil, seleccione **Propiedades**.
4. En la ventana Propiedades del dispositivo, seleccione la sección **Etiquetas**.

   Se mostrará una lista de etiquetas asignadas al dispositivo seleccionado, así como la forma en que se asignó la etiqueta: manualmente o por regla.
5. Si es necesario, realice una de las siguientes acciones:
   - Para empezar con la instalación de reglas de etiquetado, haga clic en el enlace **Configurar reglas de etiquetado automático** (solo para Windows).
   - Para renombrar una etiqueta, seleccione una y haga clic en el botón **Cambiar nombre**.
   - Para eliminar una etiqueta, seleccione una y haga clic en el botón **Eliminar**.
   - Para agregar una etiqueta manualmente, entre un en el campo en la parte inferior de la sección **Etiquetas** y haga clic en el botón **Agregar**.
6. Haga clic en el botón **Aplicar** si ha hecho cambios en la sección **Etiquetas** para que estos se apliquen.
7. Haga clic en **Aceptar**.

Si eliminara o renombrara una etiqueta en las propiedades del dispositivo, este cambio no afectará las reglas de etiquetado que han estado configuradas en las propiedades del Servidor de administración. El cambio solo se aplicará al dispositivo a cuyas propiedades se ha hecho.

## Diagnóstico remoto de dispositivos cliente. Utilidad de diagnóstico remoto de Kaspersky Security Center

La utilidad para diagnóstico remoto de Kaspersky Security Center (de aquí en adelante, utilidad de diagnóstico remoto) está diseñada para la ejecución remota de las siguientes operaciones en dispositivos cliente:

- Activación y desactivación del seguimiento, cambio del nivel de seguimiento, descarga del archivo de seguimiento.
- Descarga de información del sistema y configuración de la aplicación.
- Descarga de registros de eventos.

- Creación de un archivo de volcado para una aplicación.
- Inicio del diagnóstico y descarga de informes de diagnóstico.
- Inicio y detención de aplicaciones.

Puede utilizar los registros de eventos y los informes de diagnóstico descargados de un dispositivo cliente para solucionar problemas por cuenta propia. Además, un especialista del Servicio de soporte técnico de Kaspersky puede pedirle que descargue archivos de seguimiento, archivos de volcado, registros de eventos e informes de diagnóstico desde un dispositivo cliente para su análisis posterior en Kaspersky.

La utilidad de diagnóstico remoto se instala en el dispositivo automáticamente junto con la Consola de administración.

## Conexión de la utilidad de diagnóstico remoto a un dispositivo cliente

*Para conectar la utilidad de diagnóstico remoto a un dispositivo cliente:*

1. Seleccione algún grupo de administración del árbol de consola.
2. En el espacio de trabajo, en la pestaña **Dispositivos**, en el menú contextual de cualquier dispositivo, seleccione **Herramientas personalizadas → Diagnóstico remoto**.

   Se abre la ventana principal de la utilidad de diagnósticos remotos.
3. En el primer campo de la ventana principal de la utilidad de diagnósticos remotos, especifique qué herramientas desea utilizar para conectarse al dispositivo:
   - **Acceso mediante la Red de Microsoft Windows**.
   - **Acceso mediante el Servidor de administración**.
4. Si seleccionó **Acceso mediante la Red de Microsoft Windows** en el primer campo de la ventana principal de la utilidad, realice las siguientes acciones:
   - En el campo **Dispositivo**, especifique la dirección del dispositivo al que tiene que conectarse.

     Puede utilizar una dirección IP, un nombre NetBIOS o DNS como dirección del dispositivo.

     El valor predeterminado es la dirección del dispositivo del menú contextual en el cual se inició la utilidad.
   - Especificar cuenta para conectarse al dispositivo:
     - **Conectar como usuario actual** (seleccionado de forma predeterminada). Conéctese mediante la cuenta de usuario actual.
     - **Utilizar el nombre de usuario y la contraseña proporcionados para conectar**. Conéctese mediante una cuenta de usuario proporcionada. Especifique el **Nombre de usuario** y la **Contraseña** de la cuenta requerida.

     La conexión a un dispositivo solo es posible bajo la cuenta del administrador local del dispositivo.

5. Si en el primer campo de la ventana principal de la utilidad se ha seleccionado **Acceso mediante el Servidor de administración**, realice las siguientes acciones:

   - En el campo **Servidor de administración**, especifique la dirección del Servidor de administración desde la cual intenta conectarse al dispositivo.

     Puede utilizar una dirección IP, un nombre NetBIOS o DNS como dirección del servidor.

     El valor predeterminado es la dirección del Servidor de administración desde el que se ejecuta la utilidad.

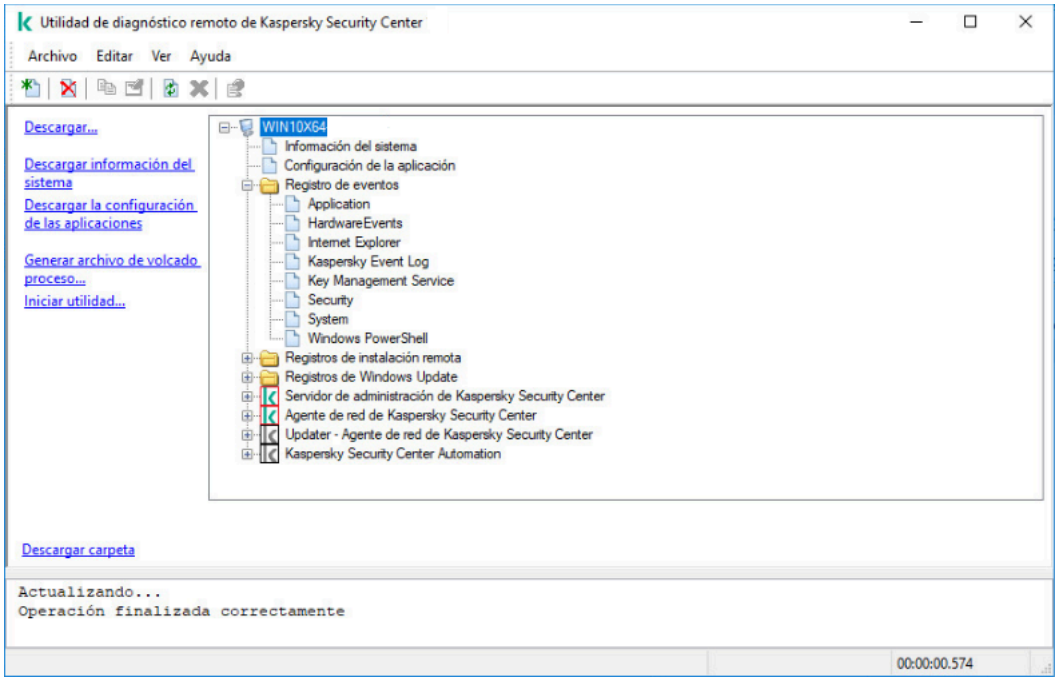
   - Si es necesario, seleccione las casillas de verificación **Usar SSL**, **Comprimir tráfico** y **El dispositivo pertenece a un Servidor de administración secundario**.

     Si está marcada la casilla **El dispositivo pertenece a un Servidor de administración secundario**, podrá completar el campo **El dispositivo pertenece a un Servidor de administración secundario** con el nombre del Servidor de administración secundario que administra el dispositivo haciendo clic en el botón **Examinar**.

6. Para conectarse al dispositivo, haga clic en el botón **Entrar**.

Debe realizar la autorización mediante la verificación en dos pasos si está habilitada para su cuenta.

De esta forma se abrirá la ventana del dispositivo para realizar el diagnóstico remoto (consulte la figura siguiente). La parte izquierda de la ventana tiene unos enlaces a las operaciones de diagnóstico del dispositivo. La parte derecha de la ventana tiene el árbol de objetos del dispositivo con el que puede operar la utilidad. La parte inferior de la ventana muestra el progreso de las operaciones de la utilidad.




Utilidad de diagnósticos remotos. Ventana de diagnósticos de dispositivo remotos

La utilidad de diagnósticos remotos guarda los archivos descargados de dispositivos al escritorio del dispositivo desde el que se haya iniciado.

## Crear un archivo de volcado para una aplicación

El archivo de volcado de una aplicación le permite ver los parámetros de la aplicación que se ejecuta en un dispositivo cliente en un momento determinado. Este archivo también contiene información sobre los módulos que se cargaron para una aplicación.

No se admite la recopilación de volcados de dispositivos con Linux.

Para recopilar volcados mediante diagnósticos remotos, se utiliza la utilidad kldumper. Esta utilidad está diseñada para recopilar los volcados de procesos de aplicaciones de Kaspersky a pedido de los especialistas del servicio de soporte técnico. Puede encontrar información detallada sobre los requisitos para usar la utilidad kldumper en la Base de conocimientos de Kaspersky Security Center.

*Si desea crear un archivo de volcado para una aplicación:*

1. En el espacio de trabajo de la carpeta **Dispositivos administrados**, en la pestaña **Dispositivos**, abra el menú contextual del dispositivo necesario y seleccione **Herramientas personalizadas** → **Diagnóstico remoto**.

   Se abre la ventana **Utilidad de diagnóstico remoto de Kaspersky Security Center**.

2. Conecte la utilidad de diagnóstico remoto a un dispositivo cliente.

   De esta forma, se abrirá la ventana para el diagnóstico remoto del dispositivo.

3. En la parte izquierda de la ventana, haga clic en el vínculo **Generar archivo de volcado de un proceso**.

4. En la ventana **Generación de proceso de volcado de memoria** que se abre, especifique el archivo ejecutable de la aplicación para la que desea generar un archivo de volcado.

5. Haga clic en el botón **Aceptar**.

Se descargará un archivo de volcado de la aplicación especificada.

Si la aplicación especificada no se está ejecutando en el dispositivo cliente, la carpeta "result" en el archivo descargado estará vacía.

Si la aplicación especificada está en ejecución, pero la descarga falla por un error o la carpeta "result" en el archivo descargado está vacía, consulte la Base de conocimientos de Kaspersky Security Center.

## Activar y desactivar el seguimiento, descargar el archivo de seguimiento

*Para activar el seguimiento en un dispositivo remoto:*

1. Ejecute la utilidad de diagnóstico remoto y conecte al dispositivo requerido.
2. En el árbol de objetos del dispositivo, seleccione la aplicación para la que desea habilitar el seguimiento.

   El seguimiento se puede activar y desactivar para aplicaciones con protección automática solo si el dispositivo está conectado mediante herramientas del Servidor de administración.

   Si desea habilitar el seguimiento para el Agente de red, también puede hacerlo creando la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades. En este caso, el Agente de red escribirá la información de seguimiento incluso si el seguimiento está desactivado para el Agente de red en la utilidad de diagnóstico remoto.

3. Para habilitar el seguimiento:

   a. En la parte izquierda de la ventana de utilidad de diagnóstico remoto, haga clic en **Habilitar seguimiento**.

   b. En la ventana **Seleccionar nivel de seguimiento**, recomendamos que mantenga los valores de configuración predeterminados. De ser necesario, un especialista del servicio de soporte técnico le indicará cómo modificar la configuración. Las opciones de configuración disponibles son las siguientes:

   - **Nivel de seguimiento**

     El nivel de seguimiento determina qué tan detallado es el archivo de seguimiento.

   - **Seguimiento con rotación** (disponible solo para Kaspersky Endpoint Security)

     La información de seguimiento se sobrescribe para que el archivo de seguimiento no aumente de tamaño desmedidamente. Especifique el número máximo de archivos que se utilizarán para almacenar la información de seguimiento y el tamaño máximo de cada archivo. Una vez que se haya guardado el número máximo de archivos de seguimiento, cada cual con su tamaño máximo, se eliminará el archivo de seguimiento más antiguo para que se pueda guardar un nuevo archivo de seguimiento.

   c. Haga clic en **Aceptar**.

4. Si utiliza Kaspersky Endpoint Security, un especialista de nuestro servicio de soporte técnico podría pedirle que habilite el seguimiento con Xperf. Esta función permite obtener información sobre el rendimiento del sistema.

   Para habilitar el seguimiento con Xperf:

   a. En la parte izquierda de la ventana de la utilidad de diagnóstico remoto, haga clic en **Habilitar seguimiento con Xperf**.

   b. En la ventana **Seleccionar nivel de seguimiento** que se abre, dependiendo de la solicitud del especialista del Servicio de soporte técnico, seleccione uno de los siguientes niveles de seguimiento:

   - **Nivel bajo**

     Un archivo de seguimiento de este tipo contiene una cantidad mínima de información sobre el sistema.

     Esta opción está seleccionada de forma predeterminada.

   - **Nivel profundo**

     Un archivo de seguimiento de este tipo contiene información más detallada que los archivos de seguimiento que se generan cuando se elige la opción *Nivel bajo*. El especialista en soporte técnico podría pedirle que elija este nivel si la información contenida en un archivo de nivel bajo no basta para evaluar el rendimiento del sistema. Un archivo de seguimiento de *Nivel profundo* contiene distintas clases de información técnica sobre el sistema: información sobre el hardware, el sistema operativo, la lista de procesos y programas iniciados y finalizados, los eventos utilizados para la evaluación del rendimiento, eventos de la Herramienta de evaluación del sistema de Windows y más.

   c. Seleccione uno de los siguientes tipos de seguimiento:

   - **Tipo básico**

La información de seguimiento se obtendrá mientras Kaspersky Endpoint Security esté en funcionamiento.

Esta opción está seleccionada de forma predeterminada.

- **Tipo con reinicio**

  La información de seguimiento se obtendrá cuando se inicie el sistema operativo del dispositivo administrado. Este tipo de seguimiento es efectivo cuando el problema que afecta al rendimiento del sistema ocurre después de encender el dispositivo y antes de que se inicie Kaspersky Endpoint Security.

d. También podrían pedirle que habilite la opción **Seguimiento con rotación** para evitar que el archivo de seguimiento aumente de tamaño desmedidamente. Si habilita esta opción, especifique el tamaño que el archivo de seguimiento podrá tener como máximo. Cuando el archivo alcance su máximo tamaño, la información de seguimiento más antigua comenzará a reemplazarse con información nueva.

e. Haga clic en **Aceptar**.

En algunos casos, para habilitar el seguimiento, deberá reiniciar la aplicación de seguridad y su tarea.

La utilidad de diagnóstico remoto permite realizar el seguimiento de la aplicación seleccionada.

*Para descargar un archivo de seguimiento de una aplicación:*

1. Ejecute la utilidad de diagnóstico remoto y conéctela al dispositivo necesario, tal y como se describe en "Conexión de la utilidad de diagnóstico remoto a un dispositivo cliente".
2. En el nodo de la aplicación, en la carpeta **Archivos de seguimiento**, seleccione el archivo deseado.
3. En la parte izquierda de la ventana de la utilidad de diagnóstico remoto, haga clic en **Descargar archivo completo**.

   Para archivos de gran tamaño se pueden descargar las partes de rastreo más recientes.

   Puede eliminar el archivo de seguimiento resaltado. El archivo puede eliminarse una vez que el seguimiento se ha deshabilitado.

El archivo seleccionado se descarga en la ubicación especificada en la parte inferior de la ventana.

*Para desactivar el seguimiento en un dispositivo remoto:*

1. Ejecute la utilidad de diagnóstico remoto y conéctela al dispositivo necesario, tal y como se describe en "Conexión de la utilidad de diagnóstico remoto a un dispositivo cliente".
2. En el árbol de objetos del dispositivo, seleccione la aplicación para la que desea deshabilitar el seguimiento.

   El seguimiento se puede activar y desactivar para aplicaciones con protección automática solo si el dispositivo está conectado mediante herramientas del Servidor de administración.

3. En la parte izquierda de la ventana de la utilidad de diagnóstico remoto, haga clic en **Deshabilitar seguimiento**.

La utilidad de diagnóstico remoto desactiva el seguimiento para la aplicación seleccionada.

## Descargar la configuración de las aplicaciones

*Para descargar la configuración de la aplicación desde un dispositivo remoto:*

1. Ejecute la utilidad de diagnóstico remoto y conéctela al dispositivo necesario, tal y como se describe en "Conexión de la utilidad de diagnóstico remoto a un dispositivo cliente".

2. En el árbol de objetos de la ventana de utilidad de diagnóstico remoto, seleccione el nodo superior con el nombre del dispositivo.

3. En la parte izquierda de la ventana de utilidad de diagnóstico remoto, seleccione la acción que necesita de las siguientes opciones:

   - **Descargar información del sistema**
   - **Descargar configuración de las aplicaciones**
   - **Generar archivo de volcado de un proceso**

     En la ventana que se abrirá al hacer clic en este enlace, especifique el archivo ejecutable de la aplicación para la cual necesita generar un archivo de volcado.

   - **Iniciar utilidad**

     En la ventana que se abre después de hacer clic en este enlace, especifique el archivo ejecutable de la utilidad que desea iniciar y su configuración de ejecución.

La utilidad seleccionada se descarga y se inicia en el dispositivo.

## Descargar registros de eventos

*Para descargar un registro de eventos de un dispositivo remoto:*

1. Ejecute la utilidad de diagnóstico remoto y conéctela al dispositivo necesario, tal y como se describe en "Conexión de la utilidad de diagnóstico remoto a un dispositivo cliente".

2. En la carpeta **Registros Eventos del sistema** del árbol de objetos del dispositivo, seleccione el registro correspondiente.

3. Descargue el registro seleccionado haciendo clic en el enlace **Descargar el registro de eventos <nombre del registro de eventos>** en la parte izquierda de la ventana de utilidad de diagnóstico remoto.

El registro de eventos seleccionado se descarga en la ubicación especificada en el panel inferior.

## Descarga de varios elementos de información de diagnóstico

La utilidad de diagnóstico remoto de Kaspersky Security Center le permite descargar múltiples elementos de información de diagnóstico, incluidos registros de eventos, información del sistema, archivos de seguimiento y archivos de volcado.

*Para descargar información de diagnóstico desde un dispositivo remoto:*

1. Ejecute la utilidad de diagnóstico remoto y conéctela al dispositivo necesario, tal y como se describe en "Conexión de la utilidad de diagnóstico remoto a un dispositivo cliente".
2. En la parte izquierda de la ventana de utilidad de diagnóstico remoto, haga clic en **Descargar**.
3. Seleccione las casillas al lado de los elementos que desea descargar.
4. Haga clic en **Iniciar**.

Cada elemento seleccionado se descarga en la ubicación especificada en el panel inferior.

## Inicio de los diagnósticos y descarga de los resultados

*Para realizar un diagnóstico de una aplicación instalada en un dispositivo remoto y descargar los resultados:*

1. Ejecute la utilidad de diagnóstico remoto y conéctela al dispositivo necesario, tal y como se describe en "Conexión de la utilidad de diagnóstico remoto a un dispositivo cliente".
2. En el árbol de objetos del dispositivo, seleccione la aplicación necesaria.
3. Inicie el diagnóstico haciendo clic en el enlace **Ejecutar diagnóstico** en la parte izquierda de la ventana de utilidad de diagnóstico remoto.

   Aparece un informe de diagnóstico en el nodo de la aplicación seleccionada en el árbol de objeto.
4. Seleccione el informe de diagnóstico recién generado en el árbol de objetos y descárguelo mediante un clic en el enlace **Descargar carpeta**.

El informe seleccionado se descarga en la ubicación especificada en el panel inferior.

## Iniciar, detener y reiniciar aplicaciones

Puede iniciar, detener y reiniciar aplicaciones si ha conectado el dispositivo mediante herramientas del Servidor de administración.

*Para iniciar, detener o reiniciar una aplicación:*

1. Ejecute la utilidad de diagnóstico remoto y conéctela al dispositivo necesario, tal y como se describe en "Conexión de la utilidad de diagnóstico remoto a un dispositivo cliente".
2. En el árbol de objetos del dispositivo, seleccione la aplicación necesaria.
3. Seleccione una acción en la parte izquierda de la ventana de utilidad de diagnóstico remoto:
   - **Detener la aplicación**
   - **Reiniciar aplicación**
   - **Iniciar la aplicación**

De acuerdo con la acción seleccionada, la aplicación se iniciará, se detendrá o se reiniciará.

# Dispositivos con protección de UEFI

El *Dispositivo con protección de UEFI* es un dispositivo que tiene una aplicación o solución de Kaspersky para UEFI integrada al nivel de BIOS. La protección integrada garantiza que el dispositivo está protegido desde el momento en que se lo enciende. La protección en dispositivos sin software integrado, por el contrario, no comienza a funcionar sino hasta que la aplicación de seguridad se inicia. Kaspersky Security Center admite la administración de estos dispositivos.

*Para modificar la configuración de conexión de los dispositivos con protección de UEFI, realice lo siguiente:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
3. En la ventana de propiedades del Servidor de administración, seleccione **Configuración de conexión del servidor** → **Puertos adicionales**.
4. En la sección **Puertos adicionales**, modifique la configuración correspondiente:
   - **Abrir puerto para dispositivos con protección de UEFI y dispositivos con KasperskyOS**

     Los dispositivos con protección de UEFI podrán conectarse al Servidor de administración.

   - **Puerto para dispositivos con protección de UEFI y dispositivos con KasperskyOS**

     Puede cambiar el número de puerto si la opción **Abrir puerto para dispositivos con protección de UEFI y dispositivos con KasperskyOS** está habilitada. El número de puerto predeterminado es 13294.
5. Haga clic en **Aceptar**.

# Configuración de un dispositivo administrado

*Para ver la configuración de un dispositivo administrado:*

1. En el árbol de consola, seleccione la carpeta **Dispositivos administrados**.
2. En el espacio de trabajo de la carpeta, seleccione un dispositivo.
3. En el menú contextual del dispositivo, seleccione **Propiedades**.

Se abre la ventana de propiedades del dispositivo elegido, con la sección **General** seleccionada.

## General

La sección **General** muestra información general sobre el dispositivo cliente. La información se basa en los datos recibidos durante la última sincronización del dispositivo cliente con el Servidor de administración.

- **Nombre**

  En este campo, puede ver y modificar el nombre asignado al dispositivo cliente en el grupo de administración.

- **Descripción**

  En este campo, puede ingresar una descripción adicional para el dispositivo cliente.

- **Dominio de Windows**

  Dominio o grupo de trabajo de Windows en el que está incluido el dispositivo.

- **Nombre NetBIOS**

  Nombre de la red de Windows del dispositivo cliente.

- **Nombre DNS**

  Nombre del dominio DNS del dispositivo cliente.

- **Dirección IP**

  Dirección IP del dispositivo.

- **Grupo**

  Grupo de administración en el que está incluido el dispositivo cliente.

- **Última actualización**

  Fecha en que las bases de datos o las aplicaciones del antivirus se actualizaron por última vez en el dispositivo.

- **Visible por última vez**

  Fecha y hora en que el dispositivo se vio en la red por última vez.

- **Conectado al Servidor de administración**

  Fecha y hora en que el Agente de red instalado en el dispositivo cliente se conectó al Servidor de administración por última vez.

- **No desconectar del Servidor de administración**

  Si esta opción está habilitada, se mantendrá una conexión continua entre el dispositivo administrado y el Servidor de administración. Esta opción podría resultarle útil si no usa servidores push, que proporcionan este tipo de conectividad.

  Si no habilita esta opción y no utiliza servidores push, el dispositivo administrado se conectará al Servidor de administración únicamente para sincronizar o transmitir información.

  El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

  Esta opción está deshabilitada de manera predeterminada en los dispositivos administrados. Esta opción está habilitada de manera predeterminada en el dispositivo en el que se ha instalado el Servidor de administración y no se puede deshabilitar en ese caso.

## Protección

La sección **Protección** proporciona información sobre el estado actual de la protección antivirus en el dispositivo cliente:

- **Estado del dispositivo**

  Estado del dispositivo cliente, asignado sobre la base de los criterios definidos por el administrador para el estado de protección antivirus del dispositivo y la actividad del dispositivo en la red.

- **Todos los problemas**

  Tabla con una lista en la que se enumeran los problemas detectados por las aplicaciones administradas del dispositivo cliente. Cada problema está acompañado del estado que la aplicación sugiere asignar al dispositivo a raíz del problema.

- **Protección en tiempo real**

  Este campo muestra el estado de la protección en tiempo real registrado en el dispositivo cliente.

  Si el estado se modifica en el dispositivo, el cambio no se verá reflejado en la ventana de propiedades del dispositivo sino hasta que el dispositivo se sincronice con el Servidor de administración.

- **Último análisis a pedido**

  Fecha y hora del último análisis antimalware realizado en el dispositivo cliente.

- Número total de amenazas detectadas

  Cantidad total de amenazas detectadas en el dispositivo cliente desde la instalación de la aplicación de seguridad (primer análisis) o desde la última vez que el contador de amenazas se puso en cero.

- Amenazas activas

  Número de archivos no procesados en el dispositivo cliente.

  Este campo no refleja el número de archivos no procesados en dispositivos móviles.

- Estado de cifrado del disco

  Estado del cifrado de archivos en las unidades locales del dispositivo. Para obtener una descripción de los estados, consulte la Ayuda de Kaspersky Endpoint Security para Windows.

## Aplicaciones

La sección **Aplicaciones** enumera todas las aplicaciones de Kaspersky que se encuentran instaladas en el dispositivo cliente. Esta sección contiene el botón de inicio (  ) y el botón de parada (  ) que le permiten iniciar y detener la aplicación de Kaspersky seleccionada (sin incluir el Agente de red). Puede usar estos botones si el puerto 15000 UDP está disponible en el dispositivo administrado para recibir notificaciones push del Servidor de administración. Si el dispositivo administrado no está disponible para notificaciones push, pero el modo de conexión continua al Servidor de administración está habilitado (la opción **No desconectar del Servidor de administración** en la sección **General** está habilitada), los botones Iniciar y Detener también están disponibles. Además, la sección **Aplicaciones** contiene los siguientes botones:

- Eventos

  Haga clic en este botón para ver una lista de los eventos ocurridos en el dispositivo cliente durante el funcionamiento de la aplicación y para ver los resultados de la tarea de esa aplicación.

- Estadísticas

  Haga clic en este botón para ver información estadística actualizada sobre la aplicación.

- Propiedades

  Haga clic en este botón para recibir información acerca de la aplicación y para configurar la aplicación.

## Tareas

La pestaña **Tareas** permite administrar las tareas del dispositivo cliente. Utilice esta sección para crear tareas nuevas, ver la lista de tareas existentes, ver los resultados de ejecución de las tareas e iniciar, detener, eliminar y reconfigurar las tareas existentes. La lista de tareas mostrada se basa en los datos recibidos durante la última sesión de sincronización entre el cliente y el Servidor de administración. El Servidor de administración solicita detalles sobre el estado de las tareas al dispositivo cliente.

Puede usar los botones Iniciar (  ), Detener (  ) y Eliminar (  ) si el puerto 15000 UDP está disponible en el dispositivo administrado para recibir notificaciones push del Servidor de administración. Si el dispositivo administrado no está disponible para notificaciones push, pero el modo de conexión continua al Servidor de administración está habilitado (la opción **No desconectar del Servidor de administración** en la sección **General** está habilitada), los botones Iniciar, Detener y Eliminar también están disponibles.

Si no se establece una conexión, no se muestra el estado de la tarea y los botones quedan deshabilitados.

## Eventos

La pestaña **Eventos** muestra los eventos registrados en el Servidor de administración para el dispositivo cliente seleccionado.

## Etiquetas

La pestaña **Etiquetas** permite administrar la lista de palabras clave que se utilizan para buscar dispositivos cliente. Aquí puede ver la lista de etiquetas existentes, asignar etiquetas incluidas en la lista, configurar reglas de etiquetado automático, agregar etiquetas nuevas, eliminar etiquetas antiguas y modificar el nombre de las etiquetas existentes.

## Información del sistema

La sección **Información general del sistema** brinda información sobre la aplicación instalada en el dispositivo cliente.

## Registro de aplicaciones

En la sección **Registro de aplicaciones**, puede ver un registro de las aplicaciones instaladas en el dispositivo cliente y de las actualizaciones de esas aplicaciones; también puede configurar el modo de visualización del registro de aplicaciones.

Podrá ver información sobre las aplicaciones instaladas si el Agente de red instalado en el dispositivo cliente le envía la información necesaria al Servidor de administración. Puede configurar el envío de información al Servidor de administración en la ventana de propiedades del Agente de red o en su directiva, en la sección **Repositorios**.

- **Mostrar únicamente las aplicaciones de seguridad incompatibles**

  Si habilita esta opción, la lista de aplicaciones incluirá solo aquellas aplicaciones de seguridad que sean incompatibles con las aplicaciones de Kaspersky.

  Esta opción está deshabilitada de forma predeterminada.

- **Mostrar actualizaciones**

  Si habilita esta opción, la lista de aplicaciones incluirá no solo aplicaciones, sino también los paquetes de actualización que se hayan instalado para esas aplicaciones.

  Para mostrar la lista de actualizaciones, se utilizan 100 kB de tráfico. Si cierra la lista y la abre nuevamente, se consumirán 100 kB de tráfico más.

  Esta opción está deshabilitada de forma predeterminada.

- Exportar a archivo

  Haga clic en este botón para exportar la lista de aplicaciones instaladas en el dispositivo a un archivo CSV o TXT.

- Historial

  Haga clic en este botón para ver los eventos relacionados con la instalación de aplicaciones en el dispositivo. Verá la siguiente información:

  - Fecha y hora en que la aplicación se instaló en el dispositivo
  - Nombre de la aplicación
  - Versión de la aplicación

- Propiedades

  Haga clic en este botón para ver las propiedades de la aplicación seleccionada en la lista de aplicaciones instaladas en el dispositivo. Verá la siguiente información:

  - Nombre de la aplicación
  - Versión de la aplicación
  - Proveedor de la aplicación

## Archivos ejecutables

La sección **Archivos ejecutables** muestra los archivos ejecutables almacenados en el dispositivo cliente.

## Registro de hardware

En la sección **Registro de hardware**, puede ver información sobre el hardware instalado en el dispositivo cliente. Esta información está disponible para dispositivos con Windows y Linux.

Asegúrese de que la utilidad lshw esté instalada en los dispositivos Linux desde los que desea obtener detalles del hardware. Los detalles de hardware obtenidos de las máquinas virtuales pueden estar incompletos según el hipervisor que se utilice.

Si el Agente de red está instalado en un dispositivo con Windows, envía al Servidor de administración la siguiente información sobre el hardware del dispositivo:

- RAM
- Dispositivos de almacenamiento
- Placa madre
- CPU

- Adaptadores de red
- Monitores
- Adaptador de video
- Tarjeta de sonido

Si el Agente de red está instalado en un dispositivo con Linux o macOS, envía al Servidor de administración la siguiente información sobre el hardware del dispositivo, si el sistema operativo la proporciona:

- Volumen total de la RAM
- Volumen total de los dispositivos de almacenamiento masivo
- Placa madre
- CPU
- Adaptadores de red

## Sesiones

La sección **Sesiones** se muestra solo para los dispositivos Windows y contiene información acerca del propietario del dispositivo cliente y de las cuentas de los usuarios que trabajaron con el dispositivo cliente seleccionado.

La información sobre los usuarios del dominio se genera utilizando datos de Active Directory. Los detalles de los usuarios locales son proporcionados por el Administrador de cuentas de seguridad de Windows instalado en el dispositivo cliente.

- **Propietario del dispositivo**

  El campo **Propietario del dispositivo** muestra el nombre del usuario con el que el administrador puede comunicarse cuando surge la necesidad de realizar determinadas operaciones con el dispositivo cliente.

  Use los botones **Asignar** y **Propiedades** para seleccionar el propietario del dispositivo y ver información acerca del usuario designado como propietario del dispositivo.

  Use el botón con la cruz roja para eliminar al actual propietario del dispositivo.

La lista muestra las cuentas de los usuarios que usan el dispositivo cliente.

- **Nombre**

  Nombre del dispositivo en la red de Windows.

- **Nombre del participante**

  Nombre (local o de dominio) del usuario que inició sesión en el sistema del dispositivo.

- **Cuenta**

  Cuenta del usuario que inició sesión en el dispositivo.

- **Correo electrónico**

  Dirección de correo electrónico del usuario.

- **Teléfono**

  Número de teléfono del usuario.

## Problemas de seguridad

En la pestaña **Problemas de seguridad**, puede ver, crear y editar problemas de seguridad para el dispositivo cliente. Los problemas de seguridad se pueden crear manualmente por el administrador o automáticamente por las aplicaciones de Kaspersky administradas que se han instalado en el dispositivo cliente. El administrador podría crear un problema de seguridad si, por ejemplo, algunos de sus usuarios han copiado malware de una unidad extraíble en más de una ocasión. En el texto del problema de seguridad, el administrador podría brindar una breve descripción del caso, delinear las acciones que recomienda tomar (por ejemplo, medidas disciplinarias contra los usuarios) y agregar un vínculo al usuario o a los usuarios.

Se denomina *procesado* al problema de seguridad para el cual se han tomado todas las medidas necesarias. La presencia de problemas de seguridad no procesados puede usarse como condición para cambiar el estado de un dispositivo a *Crítico* o *Advertencia*.

En esta sección, encontrará una lista con problemas de seguridad que se hayan creado para el dispositivo. Los problemas de seguridad se clasifican por tipo y por nivel de gravedad. El tipo de problema de seguridad lo define la aplicación de Kaspersky que crea el problema de seguridad. Si desea resaltar los problemas de seguridad procesados de la lista, marque la casilla de la columna **Procesado**.

## Vulnerabilidades de software

La sección **Vulnerabilidades de software** muestra información sobre las vulnerabilidades de las aplicaciones de terceros instaladas en los dispositivos cliente. Puede usar el campo de búsqueda que se encuentra sobre la lista para buscar vulnerabilidades por nombre.

- **Exportar a archivo**

  Haga clic en el botón **Exportar a archivo** para guardar la lista de vulnerabilidades en un archivo. De manera predeterminada, la aplicación exporta la lista de vulnerabilidades a un archivo CSV.

- **Mostrar solo las vulnerabilidades que pueden repararse**

  Si habilita esta opción, la sección mostrará las vulnerabilidades que se puedan reparar con un parche.

  Si deshabilita esta opción, la sección mostrará tanto las vulnerabilidades que se puedan reparar con un parche como las vulnerabilidades para las que no exista parche publicado.

  Esta opción está activada de forma predeterminada.

- **Propiedades**

  Seleccione una vulnerabilidad de software en la lista y haga clic en el botón **Propiedades** para ver las propiedades de esa vulnerabilidad en una ventana separada. En la ventana, puede hacer lo siguiente:

  - Ignorar la vulnerabilidad de software en el dispositivo administrado (en la Consola de administración o en Kaspersky Security Center Web Console).
  - Ver la lista de reparaciones recomendadas para la vulnerabilidad.
  - Elegir manualmente las actualizaciones de software que se usarán para corregir la vulnerabilidad (en la Consola de administración o en Kaspersky Security Center Web Console).
  - Ver las instancias de la vulnerabilidad.
  - Ver la lista de tareas existentes que permiten reparar la vulnerabilidad y crear tareas de reparación nuevas.

## Actualizaciones disponibles

Esta sección muestra las actualizaciones de software que se han encontrado en el dispositivo, pero que aún no se han instalado. La información sobre las actualizaciones opcionales de Microsoft Windows no se envía al Servidor de administración.

- **Mostrar actualizaciones instaladas**

  Si habilita esta opción, la lista mostrará tanto las actualizaciones instaladas como las que no estén instaladas en el dispositivo cliente.

  Esta opción está deshabilitada de forma predeterminada.

## Directivas activas

Esta sección contiene una lista de las directivas para aplicaciones de Kaspersky que se encuentran asignadas a este dispositivo.

- Exportar a archivo

  Haga clic en el botón **Exportar a archivo** para guardar la lista de directivas activas en un archivo. De manera predeterminada, la aplicación exporta la lista de directivas a un archivo CSV.

## Perfiles de directivas activos

- Perfiles de directivas activos

  Esta lista permite ver información sobre los perfiles de directivas que se encuentran activos en los dispositivos cliente. Para encontrar un perfil de directiva activo en la lista, escriba el nombre de una directiva o de un perfil de directiva en la barra de búsqueda que se encuentra sobre la lista.

- Exportar a archivo

  Haga clic en el botón **Exportar a archivo** para guardar la lista de perfiles de directivas activos en un archivo. De manera predeterminada, la aplicación exporta la lista de perfiles de directivas a un archivo CSV.

## Puntos de distribución

Esta sección contiene una lista de los puntos de distribución con los que interactúa el dispositivo.

- Exportar a archivo

  Haga clic en el botón **Exportar a archivo** para guardar en un archivo la lista de puntos de distribución con los que interactúa el dispositivo. De manera predeterminada, la aplicación exporta la lista de dispositivos a un archivo CSV.

- Propiedades

  Haga clic en el botón **Propiedades** para ver y configurar el punto de distribución con el que interactúa el dispositivo.

# Ajustes generales de una directiva

## General

En la sección **General**, puede modificar el estado de la directiva y especificar la herencia de la configuración de la directiva:

- A través del bloque **Estado de la directiva**, puede seleccionar uno de los modos posibles para la directiva:
  - Directiva activa

    Si se selecciona esta opción, se activa la directiva.

    Esta opción está seleccionada de forma predeterminada.
  - Directiva para fuera de la oficina

    Una directiva "fuera de la oficina" entra en vigor (es decir, se activa) cuando el dispositivo sale de la red corporativa.
  - Directiva inactiva

    Si selecciona esta opción, la directiva estará inactiva, pero quedará guardada en la carpeta **Directivas**. Podrá activarla cuando resulte necesario.
- En el grupo de ajustes **Herencia de configuración**, puede configurar las opciones de directiva:
  - Heredar configuración desde la directiva principal

    Si habilita esta opción, la directiva heredará los valores de configuración definidos en la directiva del grupo de nivel superior. Estos valores, en consecuencia, estarán bloqueados.

    Esta opción está activada de forma predeterminada.
  - Forzar la herencia de configuración en las directivas secundarias

    Si habilita esta opción, cuando modifique la directiva y se apliquen los cambios, ocurrirá lo siguiente:
    - Los valores de configuración de la directiva se propagarán a las directivas de los subgrupos de administración (es decir, a las directivas secundarias).
    - En la ventana de propiedades de cada directiva secundaria, dentro del bloque **Herencia de configuración** de la sección **General**, se habilitará automáticamente la opción **Heredar configuración de la directiva primaria**.

    Habilitar esta opción hace que los ajustes de las directivas secundarias se bloqueen.

    Esta opción está deshabilitada de forma predeterminada.

### Configuración de eventos

La sección **Configuración de eventos** le permite configurar el registro de los eventos y las notificaciones de eventos. Los eventos están distribuidos por nivel de importancia en las siguientes pestañas:

- **Crítico**

  La pestaña **Crítico** no se muestra en las propiedades de la directiva del Agente de red.

- **Error funcional**
- **Advertencia**
- **Información**

En cada pestaña, la lista muestra los tipos de eventos y el plazo de almacenamiento de eventos predeterminado en el Servidor de administración (en días). Al hacer clic en el botón **Propiedades**, podrá especificar los parámetros del registro de eventos y las notificaciones de los eventos seleccionados en la lista. De forma predeterminada, la configuración de notificación común especificada para todo el Servidor de administración se usa para todos los tipos de eventos. Sin embargo, puede cambiar configuraciones específicas para los tipos de eventos requeridos.

Por ejemplo, en la pestaña **Advertencia**, puede configurar el tipo de evento **Ocurrió un problema de seguridad**. Tales eventos pueden ocurrir, por ejemplo, cuando el espacio libre en el disco de un punto de distribución es inferior a 2 GB (se requieren al menos 4 GB para instalar aplicaciones y descargar actualizaciones de forma remota). Para configurar el evento **Ocurrió un problema de seguridad**, selecciónelo y haga clic en el botón **Propiedades**. Luego, puede especificar dónde almacenar los eventos ocurridos y cómo notificarlos.

Si el Agente de red detectó un problema de seguridad, puede administrar este problema utilizando la configuración de un dispositivo administrado.

Para seleccionar múltiples tipos de eventos, use las teclas **Mayús** o **Ctrl**; para seleccionar todos los tipos, use el botón **Seleccionar todo**.

## Ajustes de la directiva del Agente de red

*Para configurar la directiva del Agente de red:*

1. En el árbol de la consola, seleccione la carpeta **Directivas**.
2. En el espacio de trabajo de la carpeta, seleccione la directiva del Agente de red.
3. En el menú contextual de la directiva, seleccione **Propiedades**.

Se abre la ventana de propiedades de la directiva del Agente de red.

Consulte la tabla comparativa que detalla cómo se aplican las configuraciones a continuación, según el tipo de sistema operativo utilizado.

## General

En la sección **General**, puede modificar el estado de la directiva y especificar la herencia de la configuración de la directiva:

- A través del bloque **Estado de la directiva**, puede seleccionar uno de los modos posibles para la directiva:
  - **Directiva activa**

    Si se selecciona esta opción, se activa la directiva.

    Esta opción está seleccionada de forma predeterminada.

  - **Directiva para fuera de la oficina**

    Una directiva "fuera de la oficina" entra en vigor (es decir, se activa) cuando el dispositivo sale de la red corporativa.

  - **Directiva inactiva**

    Si selecciona esta opción, la directiva estará inactiva, pero quedará guardada en la carpeta **Directivas**. Podrá activarla cuando resulte necesario.

- En el grupo de ajustes **Herencia de configuración**, puede configurar las opciones de directiva:
  - **Heredar configuración desde la directiva principal**

    Si habilita esta opción, la directiva heredará los valores de configuración definidos en la directiva del grupo de nivel superior. Estos valores, en consecuencia, estarán bloqueados.

    Esta opción está activada de forma predeterminada.

  - **Forzar la herencia de configuración en las directivas secundarias**

    Si habilita esta opción, cuando modifique la directiva y se apliquen los cambios, ocurrirá lo siguiente:
    - Los valores de configuración de la directiva se propagarán a las directivas de los subgrupos de administración (es decir, a las directivas secundarias).
    - En la ventana de propiedades de cada directiva secundaria, dentro del bloque **Herencia de configuración** de la sección **General**, se habilitará automáticamente la opción **Heredar configuración de la directiva primaria**.

    Habilitar esta opción hace que los ajustes de las directivas secundarias se bloqueen.

    Esta opción está deshabilitada de forma predeterminada.

## Configuración de eventos

La sección **Configuración de eventos** le permite configurar el registro de los eventos y las notificaciones de eventos. Los eventos están distribuidos por nivel de importancia en las siguientes pestañas:

- **Crítico**

  La pestaña **Crítico** no se muestra en las propiedades de la directiva del Agente de red.

- **Error funcional**
- **Advertencia**
- **Información**

En cada pestaña, la lista muestra los tipos de eventos y el plazo de almacenamiento de eventos predeterminado en el Servidor de administración (en días). Al hacer clic en el botón **Propiedades**, podrá especificar los parámetros del registro de eventos y las notificaciones de los eventos seleccionados en la lista. De forma predeterminada, la configuración de notificación común especificada para todo el Servidor de administración se usa para todos los tipos de eventos. Sin embargo, puede cambiar configuraciones específicas para los tipos de eventos requeridos.

Por ejemplo, en la pestaña **Advertencia**, puede configurar el tipo de evento **Ocurrió un problema de seguridad**. Tales eventos pueden ocurrir, por ejemplo, cuando el espacio libre en el disco de un punto de distribución es inferior a 2 GB (se requieren al menos 4 GB para instalar aplicaciones y descargar actualizaciones de forma remota). Para configurar el evento **Ocurrió un problema de seguridad**, selecciónelo y haga clic en el botón **Propiedades**. Luego, puede especificar dónde almacenar los eventos ocurridos y cómo notificarlos.

Si el Agente de red detectó un problema de seguridad, puede administrar este problema utilizando la configuración de un dispositivo administrado.

Para seleccionar múltiples tipos de eventos, use las teclas **Mayús** o **Ctrl**; para seleccionar todos los tipos, use el botón **Seleccionar todo**.

## Configuración

En la sección **Configuración**, puede configurar la directiva del Agente de red:

- **Distribuir archivos solo a través de los puntos de distribución**

  Si se habilita esta opción, los Agentes de red en los dispositivos administrados recuperarán las actualizaciones solo de los puntos de distribución.

  Si se deshabilita esta opción, los Agentes de red en los dispositivos administrados recuperarán las actualizaciones de los puntos de distribución o del Servidor de administración.

  > Tenga en cuenta que las aplicaciones de seguridad en los dispositivos administrados recuperan las actualizaciones del conjunto de origen de la tarea de actualización para cada aplicación de seguridad. Si habilita la opción **Distribuir archivos solo a través de los puntos de distribución**, asegúrese de que Kaspersky Security Center esté configurado como origen de actualización en las tareas de actualización.

  Esta opción está deshabilitada de forma predeterminada.

- **Tamaño máximo de la cola de eventos, en MB**

  En este campo se puede especificar el espacio máximo que puede ocupar una cola de evento en la unidad.

  El valor predeterminado es de 2 megabytes (MB).

- **La aplicación podrá obtener información adicional sobre la directiva en el dispositivo**

  La aplicación de seguridad de un dispositivo administrado (por ejemplo, Kaspersky Endpoint Security para Windows) recibe, del Agente de red instalado en el mismo dispositivo, información sobre la directiva que para ella se ha aplicado. Si lo desea, puede ver esta información en la interfaz de la aplicación de seguridad.

  El Agente de red le brinda los siguientes datos a la aplicación:

  - Hora en que la directiva se entregó en el dispositivo administrado.
  - Nombre de la directiva activa que se encontraba vigente cuando la directiva se entregó en el dispositivo administrado.
  - Nombre de la directiva fuera de la oficina que se encontraba vigente cuando la directiva se entregó en el dispositivo administrado (no disponible en el Agente de red para Linux).
  - Nombre y ruta completa al grupo de administración en el que se encontraba el dispositivo administrado cuando la directiva se entregó en el dispositivo administrado.
  - Lista de perfiles de directivas activas que se encontraban vigentes cuando la directiva se entregó en el dispositivo administrado, con sus nombres y prioridades.

  Puede utilizar esta información para solucionar problemas o verificar que la directiva aplicada al dispositivo sea la esperada. Esta opción está deshabilitada de forma predeterminada.

- Evitar que el servicio del Agente de red se detenga o se elimine sin autorización e impedir cambios en su configuración

  Cuando esta opción está habilitada, una vez que el Agente de red se encuentre instalado en un dispositivo administrado, no se lo podrá eliminar ni reconfigurar a menos que se tengan los privilegios necesarios. El servicio del Agente de red no se podrá detener. Esta opción no tiene efecto en los controladores de dominio.

  Habilite esta opción para proteger el Agente de red en estaciones de trabajo operadas con derechos de administrador local.

  Esta opción está deshabilitada de forma predeterminada.

- Utilizar contraseña de desinstalación

  Si habilita esta opción y hace clic en el botón **Modificar**, podrá especificar la contraseña para la utilidad klmover y la desinstalación remota del Agente de red.

  Esta opción está deshabilitada de forma predeterminada.

## Repositorios

En la sección **Repositorios**, puede seleccionar los tipos de objetos acerca de los cuales el Agente de red enviará detalles al Servidor de administración:

- Detalles de las actualizaciones de Windows Update

  Si esta opción está habilitada, se enviará información al Servidor de administración sobre las actualizaciones de Microsoft Windows Update que deban instalarse en los dispositivos cliente.

  Aunque deshabilite esta opción, ocasionalmente encontrará actualizaciones en la sección **Actualizaciones disponibles** de las propiedades de un dispositivo. Esto podría suceder, por ejemplo, cuando los dispositivos de la organización tengan vulnerabilidades que puedan repararse con esas actualizaciones.

  Esta opción está activada de forma predeterminada. Está disponible solo para Windows.

  La información sobre las actualizaciones opcionales de Microsoft Windows no se envía al Servidor de administración.

- Detalles de las vulnerabilidades de software y las actualizaciones correspondientes

  Si esta opción está habilitada, se enviará información al Servidor de administración sobre las vulnerabilidades que se detecten en las aplicaciones de terceros instaladas en los dispositivos administrados (incluidas las aplicaciones de Microsoft) y sobre las actualizaciones disponibles para reparar vulnerabilidades en aplicaciones de terceros (excluidas, en este caso, las aplicaciones de Microsoft).

  Si habilita la opción **Detalles de las vulnerabilidades de software y las actualizaciones correspondientes**, aumentarán la carga en la red, la carga en el disco del Servidor de administración y el uso de recursos del Agente de red.

  Esta opción está activada de forma predeterminada. Está disponible solo para Windows.

  Para administrar las actualizaciones de software de Microsoft, use la opción **Detalles de las actualizaciones de Windows Update**.

- **Detalles del registro de hardware**

  Cuando el Agente de red está instalado en un dispositivo, envía información acerca del hardware de dicho dispositivo al Servidor de administración. Puede ver los detalles del hardware en las propiedades del dispositivo.

  Asegúrese de que la utilidad lshw esté instalada en los dispositivos Linux desde los que desea obtener detalles del hardware. Los detalles de hardware obtenidos de las máquinas virtuales pueden estar incompletos según el hipervisor que se utilice.

- **Detalles de las aplicaciones instaladas**

  Si se habilita esta opción, la información sobre las aplicaciones instaladas en los dispositivos cliente se enviará al Servidor de administración.

  Esta opción está activada de forma predeterminada.

- **Incluir información sobre parches**

  Se enviará información al Servidor de administración sobre los parches de las aplicaciones instaladas en los dispositivos clientes. Si habilita esta opción, podría aumentar la carga del Servidor de administración y del sistema de administración de bases de datos (DBMS). También podría aumentar el volumen de la base de datos.

  Esta opción está activada de forma predeterminada. Está disponible solo para Windows.

La directiva del Agente de red podría impedirle modificar algunos ajustes de esta sección.

## Actualizaciones y vulnerabilidades de software

En la sección **Actualizaciones y vulnerabilidades de software** puede configurar la búsqueda y distribución de actualizaciones de Windows, como también activar la búsqueda de vulnerabilidades en archivos ejecutables:

- **Usar el Servidor de administración como servidor WSUS**

  Si se habilita esta opción, las actualizaciones de Windows se descargarán al Servidor de administración. El Servidor de administración proporciona las actualizaciones descargadas a Windows Update en los dispositivos cliente en modo centralizado, mediante Agentes de red.

  Si se deshabilita esta opción, el Servidor de administración no se utilizará para descargar las actualizaciones de Windows. En tal caso, los dispositivos cliente reciben las actualizaciones de Windows por sus propios medios.

  Esta opción está deshabilitada de forma predeterminada.

- En **Permitir que los usuarios administren la instalación de actualizaciones de Windows Update**, puede limitar las actualizaciones de Windows que los usuarios podrán instalar manualmente en sus dispositivos a través de Windows Update.

  Si selecciona una nueva opción en **Permitir que los usuarios administren la instalación de actualizaciones de Windows Update** luego de que Windows Update encuentre actualizaciones para un dispositivo con Windows 10, la nueva opción no entrará en vigor sino hasta que se instalen esas actualizaciones.

  Seleccione un elemento en la lista desplegable:

  - **Permitir a los usuarios instalar todas las actualizaciones de Windows Update aplicables**

    Los usuarios podrán instalar cualquier actualización de Microsoft Windows Update que resulte adecuada para sus dispositivos.

    Seleccione esta opción si prefiere no interferir en la instalación de actualizaciones.

    Cuando un usuario instala actualizaciones de Microsoft Windows Update manualmente, puede suceder que los archivos de actualización se descarguen de los servidores de Microsoft y no del Servidor de administración. Esto puede ocurrir si el Servidor de administración no ha descargado aún esas actualizaciones. Descargar actualizaciones de los servidores de Microsoft genera tráfico adicional.

  - **Permitir a los usuarios instalar solo actualizaciones aprobadas de Windows Update**

Los usuarios podrán instalar cualquier actualización de Microsoft Windows Update que resulte adecuada para sus dispositivos y que usted haya aprobado.

Podría suceder, por ejemplo, que primero quiera instalar las actualizaciones en un entorno de prueba para verificar que no interfieran con el funcionamiento de los dispositivos, y solo entonces, en caso de no detectarse problemas, permitir que las actualizaciones aprobadas se instalen en los dispositivos cliente.

Cuando un usuario instala actualizaciones de Microsoft Windows Update manualmente, puede suceder que los archivos de actualización se descarguen de los servidores de Microsoft y no del Servidor de administración. Esto puede ocurrir si el Servidor de administración no ha descargado aún esas actualizaciones. Descargar actualizaciones de los servidores de Microsoft genera tráfico adicional.

- **No permitir que los usuarios instalen actualizaciones de Windows Update**

  Los usuarios no podrán instalar manualmente ninguna actualización de Microsoft Windows Update en sus dispositivos. Toda actualización que resulte adecuada se instalará respetando la configuración que usted defina.

  Seleccione esta opción si desea administrar la instalación de actualizaciones en forma central.

  Podría utilizar esta opción, por ejemplo, para optimizar el cronograma de instalación de actualizaciones y evitar sobrecargas en la red. Puede programar la instalación para que se lleve a cabo fuera del horario laboral a fin de no interferir con la productividad de los usuarios.

- Utilice el grupo de opciones **Modo de búsqueda de Windows Update** para seleccionar el modo de búsqueda de actualizaciones:

  - **Activo**

    Si selecciona esta opción, el Servidor de administración (asistido por el Agente de red) hará que el Agente de Windows Update del dispositivo cliente realice una solicitud al origen de actualizaciones (los servidores de Windows Update o WSUS). Tras ello, el Agente de red transmitirá al Servidor de administración la información que reciba del Agente de Windows Update.

    Esta opción solo tiene efecto si la tarea *Buscar vulnerabilidades y actualizaciones requeridas* tiene habilitada la opción **Conectarse al servidor de actualizaciones para actualizar los datos**.

    Esta opción está seleccionada de forma predeterminada.

  - **Pasivo**

    Si selecciona esta opción, el Agente de red se comunicará periódicamente con el Servidor de administración para enviarle información sobre las actualizaciones obtenidas durante la última sincronización entre el Agente de Windows Update y el origen de actualizaciones. Si el Agente de Windows Update no se sincroniza con un origen de actualizaciones, la información sobre actualizaciones del Servidor de administración se vuelve obsoleta.

    Seleccione esta opción si desea obtener actualizaciones de la caché del origen de actualizaciones.

  - **Deshabilitado**

    Si selecciona esta opción, el Servidor de administración no solicitará información sobre las actualizaciones.

    Seleccione esta opción si, por ejemplo, desea probar primero las actualizaciones en su dispositivo local.

- **Analizar los archivos ejecutables en busca de vulnerabilidades al iniciarlos**

  Si habilita esta opción, cuando se inicie un archivo ejecutable, se lo analizará en busca de vulnerabilidades.

  Esta opción está activada de forma predeterminada.

## Opciones de reinicio

En la sección **Opciones de reinicio**, puede indicar qué acción se llevará a cabo cuando se necesite reiniciar el sistema operativo de un dispositivo administrado para que una aplicación pueda instalarse, desinstalarse o utilizarse correctamente.

- **No reiniciar el sistema operativo**

  El sistema operativo no se reiniciará.

- **Reiniciar el sistema operativo automáticamente si es necesario**

  Si es necesario, el sistema operativo se reinicia de forma automática.

- **Solicitar al usuario una acción**

  La aplicación solicita al usuario que permita el reinicio del sistema operativo.

  Esta opción está seleccionada de forma predeterminada.

  - **Repetir la solicitud cada (min)**

    Si se habilita esta opción, la aplicación solicitará al usuario que permita el reinicio del sistema operativo con la frecuencia especificada en el campo que se encuentra junto a la casilla. De manera predeterminada, la frecuencia de solicitud es de 5 minutos.

    Si se deshabilita esta opción, la aplicación no solicitará reiteradamente al usuario que permita el reinicio.

    Esta opción está activada de forma predeterminada.

  - **Forzar reinicio después de (min)**

    Si se habilita esta opción, después de avisar al usuario, la aplicación forzará el reinicio del sistema operativo al finalizar el intervalo de tiempo especificado en el campo que se encuentra junto a la casilla.

    Si se deshabilita esta opción, la aplicación no forzará el reinicio.

    Esta opción está activada de forma predeterminada.

  - **Tiempo de espera antes del cierre forzado de aplicaciones en sesiones bloqueadas (min)**

    Las aplicaciones se cerrarán por la fuerza cuando el dispositivo del usuario se bloquee (sea manualmente o en forma automática tras un tiempo de inactividad).

    Si esta opción está habilitada, las aplicaciones del dispositivo bloqueado se cerrarán por la fuerza luego de transcurra el intervalo especificado en el campo de entrada.

    Si esta opción está deshabilitada, las aplicaciones del dispositivo bloqueado no se cerrarán.

    Esta opción está deshabilitada de forma predeterminada.

## Windows Desktop Sharing

En la sección **Windows Desktop Sharing**, puede activar y configurar la auditoría de las acciones del administrador que se realizan en un dispositivo remoto cuando se comparte el acceso al escritorio.

- **Habilitar auditoría**

  Habilite esta opción si desea auditar las operaciones que el administrador realice en el dispositivo remoto. Los registros de las acciones del administrador en el dispositivo remoto se computan:

  - En el registro de eventos del dispositivo remoto
  - en un archivo con la extensión syslog ubicado en la carpeta de instalación del Agente de red del dispositivo remoto
  - en la base de datos de eventos de Kaspersky Security Center

  La auditoría de las acciones del administrador está disponible cuando se cumplen las siguientes condiciones:

  - La licencia de Administración de vulnerabilidades y parches está en uso
  - El administrador tiene permiso para ejecutar el acceso compartido al escritorio del dispositivo remoto

  Si no necesita auditar las operaciones del administrador en el dispositivo remoto, no habilite esta opción.

  Esta opción está deshabilitada de forma predeterminada.

- **Máscaras de archivos cuya lectura debe monitorizarse**

  La lista contiene máscaras de archivos. Cuando la auditoría está habilitada, la aplicación monitorea los archivos de lectura del administrador que coinciden con las máscaras y guarda información sobre los archivos leídos. La lista está disponible si se ha marcado la casilla **Habilitar auditoría**. Puede editar máscaras de archivos y agregar máscaras nuevas a la lista. Cada máscara de archivo nueva se debe especificar en la lista en una línea nueva.

  De forma predeterminada, están especificadas las siguientes máscaras de archivos:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Máscaras de archivos cuya modificación debe monitorizarse**

  La lista contiene las máscaras de archivos en el dispositivo remoto. Cuando la auditoría está habilitada, la aplicación monitorea los cambios realizados por el administrador en los archivos que coinciden con las máscaras y guarda información sobre esas modificaciones. La lista está disponible si se ha marcado la casilla **Habilitar auditoría**. Puede editar máscaras de archivos y agregar máscaras nuevas a la lista. Cada máscara de archivo nueva se debe especificar en la lista en una línea nueva.

  De forma predeterminada, están especificadas las siguientes máscaras de archivos:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

## Administrar parches y actualizaciones

En la sección **Administrar parches y actualizaciones**, puede configurar la descarga y la distribución de actualizaciones, así como la instalación de parches en los dispositivos administrados:

- **Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes**

  Si esta opción está habilitada, los parches de Kaspersky con el estado de aprobación *Sin definir* se instalan automáticamente en los dispositivos administrados inmediatamente después de que se descargan de los servidores de actualizaciones.

  Si deshabilita esta opción, los parches de Kaspersky que se descarguen y que tengan el estado *Sin definir* se instalarán únicamente si cambia su estado a *Aprobada*.

  Esta opción está activada de forma predeterminada.

- **Descargar actualizaciones y bases de datos antivirus del Servidor de administración con anticipación (recomendado)**

  Si esta opción está habilitada, las actualizaciones se descargan utilizando el modelo sin conexión. Cuando el Servidor de administración recibe actualizaciones, notifica al Agente de red (en los dispositivos donde está instalado) las actualizaciones que serán necesarias para las aplicaciones administradas. Cuando el Agente de red recibe la información sobre las actualizaciones, descarga por anticipado los archivos relevantes desde el Servidor de administración. En la primera conexión con un Agente de red, el Servidor de administración inicia una descarga de actualizaciones. Después de que Agente de red descarga todas las actualizaciones a un dispositivo cliente, las actualizaciones quedan disponibles para las aplicaciones en ese dispositivo.

  Cuando una aplicación administrada de un dispositivo cliente intenta acceder al Agente de red para descargar actualizaciones, el Agente de red comprueba si tiene todas las actualizaciones necesarias. Si las actualizaciones se reciben desde el Servidor de administración no más de 25 horas antes de que la aplicación administrada las solicite, el Agente de red no se conecta al Servidor de administración, sino que proporciona actualizaciones desde el caché local a la aplicación administrada. Es posible que la conexión con el Servidor de administración no se establezca cuando el Agente de red proporciona actualizaciones para las aplicaciones en los dispositivos cliente, pero no se requiere conexión para la actualización.

  Deshabilite esta opción si prefiere no utilizar el modelo de descarga de actualizaciones sin conexión. Las actualizaciones se distribuirán siguiendo la programación de la tarea de descarga de actualizaciones.

  Esta opción está activada de forma predeterminada.

## Conectividad

La sección **Conectividad** incluye tres subsecciones anidadas:

- **Red**
- **Perfiles de conexión** (solo para Windows y macOS)
- **Programación de conexiones**

En la subsección **Red**, puede configurar la conexión con el Servidor de administración, habilitar el uso de un puerto UDP y especificar su número. Están disponibles las siguientes opciones:

- En el grupo de configuraciones **Conexión con el Servidor de administración**, puede configurar la conexión con el Servidor de administración y especificar el intervalo de tiempo para la sincronización entre dispositivos cliente y el Servidor de administración.

  - Comprimir tráfico de red

    Si esta opción está habilitada, se reducirá el volumen de datos transferido. En consecuencia, el Agente de red podrá transmitir información a mayor velocidad y el Servidor de administración deberá soportar menos carga.

    El uso de la CPU del equipo cliente podría aumentar.

    Esta casilla está activada de manera predeterminada.

  - Abrir los puertos del Agente de red en el Firewall de Microsoft Windows

    Cuando se habilita esta opción, se agregan los puertos que el Agente de red necesita para funcionar a la lista de exclusiones del Firewall de Microsoft Windows.

    Esta opción está activada de forma predeterminada.

  - Usar SSL

    Si se habilita esta opción, la conexión al Servidor de administración se establecerá a través de un puerto seguro utilizando el protocolo SSL.

    Esta opción está activada de forma predeterminada.

  - Usar la puerta de enlace de conexión en el punto de distribución (si está disponible) en la configuración de la conexión predeterminada

    Si esta opción está habilitada, la puerta de enlace de conexión del punto de distribución se usará con la configuración especificada en las propiedades del grupo de administración.

    Esta opción está activada de forma predeterminada.

- Usar puerto UDP

  Si necesita que el Agente de red se conecte al Servidor de administración a través de un puerto UDP, habilite la opción **Usar puerto UDP** y especifique un **número de puerto UDP**. Esta opción está activada de forma predeterminada. El puerto UDP predeterminado para conectarse al Servidor de administración es 15000.

- Número de puerto UDP

  En este campo, puede indicar el número del puerto UDP. El número de puerto predeterminado es 15000.

  El sistema decimal se usa para los registros.

  En dispositivos cliente con Windows XP Service Pack 2, el puerto UDP 15000 estará bloqueado por el firewall integrado. Deberá abrir el puerto manualmente.

- Utilizar el punto de distribución para forzar la conexión con el Servidor de administración

  Seleccione esta opción si seleccionó **Utilizar este punto de distribución como servidor push** en la ventana de configuración del punto de distribución. De lo contrario, el punto de distribución no funcionará como un servidor push.

En la subsección **Perfiles de conexión**, puede especificar la configuración de las ubicaciones de red, configurar perfiles de conexión para el Servidor de administración y habilitar el modo fuera de la oficina cuando el Servidor de administración no esté disponible.

- Configuración de ubicaciones de red

  La configuración de una ubicación de red define las características de la red con la cual está conectado el dispositivo cliente y especifica las reglas que hacen que el Agente de red cambie de un perfil de conexión de Servidor de administración a otro en respuesta a un cambio en las características de la red.

- Perfiles de conexión al Servidor de administración

  En esta sección, puede ver y crear los perfiles que rigen la conexión entre el Agente de red y el Servidor de administración. Desde aquí también puede crear reglas para que el Agente de red cambie a un Servidor de administración diferente cuando ocurren los siguientes eventos:

  - Cuando el dispositivo cliente se conecta a otra red local
  - Cuando el dispositivo pierde la conexión con la red local de la organización
  - Cuando se modifican la dirección de la puerta de enlace de conexión o la dirección del servidor DNS

  Los perfiles de conexión solo son compatibles con dispositivos que ejecutan Windows y MacOS.

- Habilitar el modo fuera de la oficina cuando el Servidor de administración no esté disponible

  Si se habilita esta opción, en caso de que se establezca la conexión mediante este perfil, las aplicaciones instaladas en el dispositivo cliente utilizarán perfiles de directiva para dispositivos en modo fuera de la oficina, así como directivas para fuera de la oficina. Si no hay una directiva fuera de la oficina definida para la aplicación, se utilizará la directiva activa.

  Si se deshabilita esta opción, las aplicaciones utilizarán directivas activas.

  Esta opción está deshabilitada de forma predeterminada.

En la subsección **Programación de conexiones**, puede especificar los intervalos de tiempo durante los cuales el Agente de red enviará datos al Servidor de administración:

- Conectar cuando sea necesario

  Si se selecciona esta opción, la conexión se establece cuando el Agente de red debe enviar datos al Servidor de administración.

  Esta opción está seleccionada de forma predeterminada.

- Conectarse en intervalos de tiempo especificados

  Si se selecciona esta opción, el Agente de red se conecta al Servidor de administración a una hora especificada. Puede agregar varios períodos de conexión.

## Puntos de distribución

La sección **Puntos de distribución** incluye cuatro subsecciones anidadas:

- **Sondeo de red**
- **Configuración de la conexión a Internet**
- **Proxy de KSN**
- **Actualizaciones**

En la subsección **Sondeo de red**, puede configurar el sondeo automático de la red. Puede habilitar tres tipos de sondeo, es decir, sondeo de red, sondeo de rangos IP y sondeo de Active Directory:

- Habilitar sondeo de red

  Si se habilita esta opción, el Servidor de administración sondeará automáticamente la red de acuerdo con la programación que configuró al hacer clic en los enlaces **Establecer programación de sondeo rápido** y **Establecer programación de sondeo completo**.

  Si esta opción está deshabilitada, el Servidor de administración sondeará la red con la frecuencia indicada en el campo **Frecuencia de sondeos de la red (min)**.

  El intervalo de detección de dispositivos para las versiones de Agente de red anteriores a la 10.2 se puede configurar en los campos **Frecuencia de sondeos de dominios de Windows (min)** (para el sondeo rápido de redes Windows) y **Frecuencia de sondeos de la red (min)** (para el sondeo completo de redes Windows).

  Esta opción está deshabilitada de forma predeterminada.

- Habilitar el sondeo del intervalo IP

  Si se habilita esta opción, el punto de distribución sondeará automáticamente los intervalos IP siguiendo la programación que se haya configurado tras hacer clic en el botón **Configurar programación de sondeos**.

  Si esta opción no está habilitada, el punto de distribución no hará sondeos de intervalos IP.

  La frecuencia de sondeo de rangos IP para las versiones del Agente de red anteriores a la versión 10.2 se puede configurar en el campo **Intervalo de sondeo (min)**. El campo estará disponible si se habilita la opción.

  Esta opción está deshabilitada de forma predeterminada.

- **Utilizar el sondeo Zeroconf (solo en plataformas Linux; los rangos de IP especificados manualmente serán ignorados)**

  Si esta opción está habilitada, el punto de distribución automáticamente sondea la red con dispositivos IPv6 mediante el uso de las redes de configuración cero (también denominadas *Zeroconf*). En este caso, el sondeo de rangos de IP habilitados se ignora, porque el punto de distribución sondea toda la red.

  Para empezar a usar Zeroconf, se deben cumplir las siguientes condiciones:

  - El punto de distribución debe ejecutar Linux.
  - Debe instalar la utilidad avahi-browse en el punto de distribución.

  Si esta opción está habilitada, el punto de distribución no sondea las redes con dispositivos IPv6.

  Esta opción está deshabilitada de forma predeterminada.

- **Habilitar el sondeo de Active Directory**

  Si se habilita esta opción, el Servidor de administración sondeará automáticamente Active Directory de acuerdo con la programación que configuró al hacer clic en el vínculo **Configurar programación de sondeos**.

  Si se deshabilita esta opción, el Servidor de administración no sondeará Active Directory.

  La frecuencia de sondeo de Active Directory para las versiones del Agente de red anteriores a la versión 10.2 se puede configurar en el campo **Intervalo de sondeo (min)**. El campo estará disponible si se habilita esta opción.

  Esta opción está deshabilitada de forma predeterminada.

Si sus puntos de distribución utilizan un servidor proxy al conectarse a Internet, en la subsección **Configuración de la conexión a Internet**, puede especificar la siguiente configuración:

- **Usar servidor proxy**

  Si se selecciona esta casilla, en los campos de entrada puede configurar la conexión del servidor proxy.

  Esta casilla no está marcada de manera predeterminada.

- **Dirección del servidor proxy**

  Dirección del servidor proxy.

- **Número de puerto**

  Número de puerto que se utilizará para la conexión.

- **No usar el servidor proxy para direcciones locales**

  Si habilita esta opción, no se usará un servidor proxy para establecer conexión con los dispositivos de la red local.

  Esta opción está deshabilitada de forma predeterminada.

- **Autenticación del servidor proxy**

  Si se selecciona esta casilla, en los campos de entrada se podrán especificar las credenciales para la autenticación del servidor proxy.

  Esta casilla no está marcada de manera predeterminada.

- **Nombre de usuario**

  Cuenta de usuario con la que se establece conexión con el servidor proxy.

- **Contraseña**

  Contraseña de la cuenta con la que se ejecutará la tarea.

En la subsección **Proxy de KSN**, puede configurar la aplicación para que utilice el punto de distribución para reenviar las solicitudes KSN desde los dispositivos administrados:

- **Habilitar proxy de KSN en el lado del punto de distribución**

  El servicio de proxy de KSN se ejecuta en el dispositivo que se utiliza como punto de distribución. Utilice esta función para redistribuir y optimizar el tráfico de la red.

  El punto de distribución enviará a Kaspersky las estadísticas de KSN que se enumeran en la declaración de Kaspersky Security Network. De forma predeterminada, la declaración de KSN se encuentra en %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

  Esta opción está deshabilitada de forma predeterminada. Esta opción solo se habilita si las opciones **Usar Servidor de administración como servidor proxy** y **Acepto utilizar Kaspersky Security Network** están habilitadas en la ventana de propiedades del Servidor de administración.

  Puede asignar un nodo de un clúster activo-pasivo a un punto de distribución y habilitar el servidor proxy de KSN en ese nodo.

- **Reenviar solicitudes KSN al Servidor de administración**

  El punto de distribución envía las solicitudes KSN desde los dispositivos administrados al Servidor de administración.

  Esta opción está activada de forma predeterminada.

- **Acceder a KSN en la nube/KSN directamente a través de Internet**

  El punto de distribución envía las solicitudes KSN desde los dispositivos administrados a KSN Cloud o a KPSN. Las solicitudes de KSN generadas en el punto de distribución mismo también se envían directamente a la nube de KSN Cloud o a KPSN.

  Los puntos de distribución que tienen instalado el Agente de red versión 11 (o versiones anteriores) no pueden acceder a KPSN directamente. Si desea reconfigurar los puntos de distribución para enviar solicitudes de KSN a KPSN, habilite la opción **Reenviar solicitudes KSN al Servidor de administración** para cada punto de distribución.

  Los puntos de distribución que tienen instalado el Agente de red versión 12 (o una posterior) pueden acceder a KPSN directamente.

- **Puerto TCP**

  El número del puerto de TCP que los dispositivos administrados utilizarán para conectarse al Servidor proxy de KSN. El número de puerto predeterminado es 13111.

- **Usar puerto UDP**

  Si necesita que el Agente de red se conecte al Servidor de administración a través de un puerto UDP, habilite la opción **Usar puerto UDP** y especifique un **número de puerto UDP**. Esta opción está activada de forma predeterminada. El puerto UDP predeterminado para conectarse al Servidor de administración es 15000.

En la subsección **Actualizaciones**, puede especificar si el Agente de red debe descargar archivos diff habilitando o deshabilitando la opción **Descargar archivos diff**. (De forma predeterminada, esta opción está habilitada).

### Historial de revisiones

En la pestaña **Historial de revisiones**, puede ver el historial de revisiones de la directiva del Agente de red. Allí puede comparar y ver las distintas revisiones y llevar a cabo operaciones avanzadas, como guardar revisiones en un archivo, restablecer una revisión en particular, agregar descripciones a las revisiones y editar las descripciones existentes.

# Administrar cuentas de usuario

Esta sección brinda información sobre las cuentas de usuario y los roles admitidos por la aplicación. Esta sección contiene instrucciones sobre cómo crear cuentas y roles para los usuarios de Kaspersky Security Center.

Kaspersky Security Center le permite administrar cuentas de usuario y grupos de cuentas. La aplicación admite tres tipos de cuentas:

- Cuentas de empleados de la organización. El Servidor de administración obtiene los datos de las cuentas de estos usuarios del dominio cuando sondea el controlador de dominio de la organización.
- Cuentas de usuarios locales. Cuentas locales en dispositivos administrados, así como las cuentas locales en el dispositivo en el que está el instalador del Servidor de administración.
- Cuentas de usuarios internos de Kaspersky Security Center. Puede crear cuentas de usuarios internos. Estas cuentas se utilizan solo en Kaspersky Security Center.

## Trabajar con cuentas de usuario

Kaspersky Security Center le permite administrar cuentas de usuario y grupos de cuentas. La aplicación admite dos tipos de cuentas:

- Cuentas de empleados de la organización. El Servidor de administración obtiene datos de las cuentas de estos usuarios cuando sondea la red de la organización.
- Cuentas de usuarios internos. Estas se dan cuando se administran Servidores de administración virtuales. Las cuentas de los usuarios internos se crean y utilizan solo para trabajar dentro de Kaspersky Security Center.

Puede ver la lista de cuentas de usuario de una de las siguientes maneras:

- En el árbol de la consola, vaya a **Avanzado** → **Cuentas de usuario**.
- En el árbol de la consola, vaya a **Dispositivos administrados** → pestaña **Dispositivos** → Vínculo de <nombre del dispositivo> → Sección **Sesiones**.

  En la sección **Sesiones**, se muestran las cuentas de usuario con sesiones activas en dispositivos con Windows.

La lista de cuentas de usuario se muestra correctamente si se cumplen los siguientes requisitos:

- Utilice un Agente de red de la misma versión que el Servidor de Administración o una versión posterior.
- El sondeo de Active Directory debe estar habilitado para mostrar las cuentas de los usuarios del dominio.
- En dispositivos administrados con Windows, el servicio del **Servidor (LanmanServer)** está en ejecución.

Puede realizar las siguientes acciones en las cuentas de usuario y grupos de cuentas:

- Configure los derechos de los usuarios para acceder a las características de la aplicación usando roles.
- Envíe mensajes a los usuarios mediante correo electrónico y SMS.
- Ver la lista de dispositivos móviles del usuario.
- Emitir e instalar certificados en los dispositivos móviles del usuario.
- Ver la lista de certificados emitidos para un usuario.
- Deshabilitar la verificación en dos pasos para una cuenta de usuario.

## Agregar una cuenta de un usuario interno

*Para agregar una nueva cuenta de usuario interna a Kaspersky Security Center:*

1. En el árbol de consola, abra la carpeta **Cuentas de usuario**.

   De manera predeterminada, la carpeta **Cuentas de usuario** es una subcarpeta de la carpeta **Avanzado**.
2. En el espacio de trabajo, haga clic en el botón **Agregar usuario**.

3. En la ventana **Nuevo usuario** que se abre, especifique la configuración de la nueva cuenta de usuario:

- Un nombre de usuario (  )

  > Tenga cuidado al ingresar el nombre de usuario. No podrá cambiarlo después de guardar los cambios.

- **Descripción**
- **Nombre completo**
- **Correo electrónico principal**
- **Teléfono principal**
- **Contraseña** para la conexión del usuario con Kaspersky Security Center

  La contraseña debe cumplir con las siguientes reglas:

  - La contraseña debe tener entre 8 y 256 caracteres.
  - La contraseña debe incluir caracteres de al menos tres de los grupos enumerados a continuación:
    - Letras mayúsculas (A-Z)
    - Letras minúsculas (a-z)
    - Números (0-9)
    - Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - La contraseña no debe contener espacios en blanco, caracteres Unicode o la combinación de "." y "@" cuando "." está colocado delante de "@".

  Para ver la contraseña introducida, haga clic y mantenga presionado el botón **Mostrar**.

  > El número de intentos para escribir la contraseña es limitado. De manera predeterminada, el número máximo de intentos permitidos es 10. Puede cambiar el número permitido de intentos para ingresar una contraseña, como se describe en "Cambiar el número de intentos de ingreso de contraseña permitidos".

  > Si el usuario escribe una contraseña inválida el número de veces especificado, la cuenta de usuario se bloquea durante una hora. En la lista de cuentas de usuario, el icono de usuario (  ) de una cuenta bloqueada se atenúa (no está disponible). Puede desbloquear la cuenta de usuario solo cambiando la contraseña.

- Si es necesario, seleccione la casilla de verificación **Deshabilitar cuenta** para prohibir al usuario conectarse a la aplicación. Puede deshabilitar una cuenta, por ejemplo, si desea crearla de antemano, pero activarla más tarde.
- Seleccione la casilla de verificación **Solicitar la contraseña cuando se modifique la configuración de la cuenta** si desea habilitar una opción adicional para proteger una cuenta de usuario de modificaciones no autorizadas. Si esta opción está habilitada, la modificación de la configuración de la cuenta de usuario

requiere la autorización del usuario con el derecho Modificar ACL de objeto del área funcional **Características generales: Permisos de usuario**.

4. Haga clic en **Aceptar**.

La cuenta de usuario recientemente creada se muestra en el espacio de trabajo de la carpeta **Cuentas de usuario**.

## Editar una cuenta de un usuario interno

*Modificar una cuenta de usuario interna en Kaspersky Security Center:*

1. En el árbol de consola, abra la carpeta **Cuentas de usuario**.

   De manera predeterminada, la carpeta **Cuentas de usuario** es una subcarpeta de la carpeta **Avanzado**.

2. En el espacio de trabajo, haga doble clic en la cuenta de usuario interno que desee editar.

3. En la ventana **Propiedades: <nombre de usuario>** que se abre, cambie la configuración de la cuenta de usuario:

- **Descripción**
- **Nombre completo**
- **Correo electrónico principal**
- **Teléfono principal**
- **Contraseña** para la conexión del usuario con Kaspersky Security Center

  La contraseña debe cumplir con las siguientes reglas:

  - La contraseña debe tener entre 8 y 256 caracteres.
  - La contraseña debe incluir caracteres de al menos tres de los grupos enumerados a continuación:
    - Letras mayúsculas (A-Z)
    - Letras minúsculas (a-z)
    - Números (0-9)
    - Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - La contraseña no debe contener espacios en blanco, caracteres Unicode o la combinación de "." y "@" cuando "." está colocado delante de "@".

  Para ver la contraseña introducida, haga clic y mantenga presionado el botón **Mostrar**.

  El número de intentos para escribir la contraseña es limitado. De manera predeterminada, el número máximo de intentos permitidos es 10. Puede cambiar el número permitido de intentos para ingresar una contraseña, como se describe en "Cambiar el número de intentos de ingreso de contraseña permitidos".

  Si el usuario escribe una contraseña inválida el número de veces especificado, la cuenta de usuario se bloquea durante una hora. En la lista de cuentas de usuario, el icono de usuario (  ) de una cuenta bloqueada se atenúa (no está disponible). Puede desbloquear la cuenta de usuario solo cambiando la contraseña.

- Si es necesario, seleccione la casilla de verificación **Deshabilitar cuenta** para prohibir al usuario conectarse a la aplicación. Puede desactivar una cuenta, por ejemplo, después de que un empleado abandone la empresa.
- Seleccione la opción **Solicitar la contraseña cuando se modifique la configuración de la cuenta** si desea habilitar una opción adicional para proteger una cuenta de usuario de modificaciones no autorizadas. Si esta opción está habilitada, la modificación de la configuración de la cuenta de usuario requiere la autorización del usuario con el derecho Modificar ACL de objeto del área funcional **Características generales: Permisos de usuario**.

4. Haga clic en **Aceptar**.

La cuenta de usuario editada se mostrará en el espacio de trabajo de la carpeta **Cuentas de usuario**.

# Cambiar el número de intentos de entrada de contraseña permitidos

El usuario de Kaspersky Security Center puede introducir una contraseña no válida un número limitado de veces. Una vez que se alcanza el límite, la cuenta de usuario se bloquea durante una hora.

De forma predeterminada, el número máximo de intentos permitidos para introducir una contraseña es 10. Puede cambiar el número de intentos de entrada de contraseña permitidos, como se describe en esta sección.

*Para cambiar el número de intentos de entrada de contraseña permitidos*

1. Abra el registro del sistema del dispositivo en el que está instalado el Servidor de administración (por ejemplo, de forma local con el comando regedit en el menú **Iniciar** → **Ejecutar**).
2. Vaya a la siguiente clave:
   - Para sistemas de 32 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
   - Para sistemas de 64 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF
3. Si el valor SrvSplPpcLogonAttempts no está presente, créelo. El tipo del valor es DWORD.

   De forma predeterminada, este valor no se crea después de que Kaspersky Security Center se instala.
4. Especifique el número requerido de intentos en el valor de SrvSplPpcLogonAttempts.
5. Haga clic en **Aceptar** para guardar los cambios.
6. Reinicie el servicio del Servidor de administración.

Se cambia el número máximo de intentos de entrada de contraseña permitidos.

# Configurar la verificación de que el nombre de un usuario interno sea único

Puede configurar la comprobación del nombre de un usuario interno de Kaspersky Security Center para confirmar que es único cuando este nombre se agrega a la aplicación. La comprobación del nombre de un usuario interno para confirmar que es único solo se puede realizar en un Servidor de administración virtual o en el Servidor de administración principal para el cual se está creando la cuenta de usuario, o en todos los Servidores de administración virtuales y en el Servidor de administración principal. De manera predeterminada, el nombre de un usuario interno se comprueba para confirmar que es único en todos los Servidores de administración virtuales y en el Servidor de administración principal.

*Para habilitar la comprobación del nombre de un usuario interno para confirmar que es único en un Servidor de administración virtual o en el Servidor de administración principal:*

1. Abra el registro del sistema del dispositivo en el que está instalado el Servidor de administración (por ejemplo, de forma local con el comando regedit en el menú **Iniciar** → **Ejecutar**).

2. Vaya al siguiente archivo:

   - Para sistemas de 32 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

   - Para sistemas de 64 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

3. Para la clave LP_InterUserUniqVsScope (DWORD), establezca el valor 00000001.

   El valor predeterminado especificado para esta clave es 0.

4. Reinicie el servicio del Servidor de administración.

El nombre solo se comprobará para confirmar que es único en el Servidor de administración virtual en el cual el usuario interno se creó, o en el Servidor de administración principal si el usuario interno se creara en el Servidor de administración principal.

*Para habilitar la comprobación del nombre de un usuario interno para confirmar que es único en todos los Servidores de administración virtuales o en el Servidor de administración principal:*

1. Abra el registro del sistema del dispositivo en el que está instalado el Servidor de administración (por ejemplo, de forma local con el comando regedit en el menú **Iniciar** → **Ejecutar**).

2. Vaya al siguiente archivo:

   - Para sistemas de 64 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

   - Para sistemas de 32 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

3. Para la clave LP_InterUserUniqVsScope (DWORD), establezca el valor 00000000.

   El valor predeterminado especificado para esta clave es 0.

4. Reinicie el servicio del Servidor de administración.

La comprobación del nombre para confirmar que es único se realizará en todos los Servidores de administración virtuales o en el Servidor de administración principal:

## Agregar un grupo de seguridad

Puede agregar grupos de seguridad (grupos de usuarios), establecer una configuración flexible de grupos y acceso de grupos de usuarios a varias características de la aplicación. A los grupos de seguridad se les pueden asignar nombres que se correspondan con sus respectivos propósitos. Por ejemplo, el nombre puede indicar en qué parte de la oficina se encuentran los usuarios o el nombre de la unidad organizativa de la empresa a la que pertenecen.

Un usuario puede formar parte de varios grupos de seguridad. Una cuenta de usuario administrada por un Servidor de administración virtual solo puede pertenecer a grupos de seguridad de este Servidor virtual y tener derechos de acceso solo dentro de este Servidor virtual.

*Agregar un grupo de seguridad:*

1. En el árbol de consola, seleccione la carpeta **Cuentas de usuario**.

   De manera predeterminada, la carpeta **Cuentas de usuario** es una subcarpeta de la carpeta **Avanzado**.

2. Haga clic en el botón **Agregar grupo de seguridad**.

   Se abre la ventana **Agregar grupo de seguridad**.

3. En la ventana **Agregar grupo de seguridad**, en la sección **General**, especifique el nombre del grupo.

   Un nombre de grupo no puede tener más que 255 caracteres de largo ni contener símbolos especiales como *, <, >, ?, \, :, |. El nombre del grupo debe ser exclusivo.

   Puede ingresar la descripción del grupo en el campo de entrada **Descripción**. Completar el campo **Descripción** es opcional.

4. Haga clic en **Aceptar**.

El grupo de seguridad que agregó aparece en la carpeta **Cuentas de usuario** del árbol de consola. Puede agregar usuarios al grupo recién creado.

## Agregar un usuario a un grupo

*Para agregar un usuario a un grupo:*

1. En el árbol de consola, seleccione la carpeta **Cuentas de usuario**.

   De manera predeterminada, la carpeta **Cuentas de usuario** es una subcarpeta de la carpeta **Avanzado**.

2. En la lista de grupos y cuentas de usuario, seleccione el grupo al que desea agregar al usuario.

3. En la ventana de propiedades del grupo, seleccione la sección **Usuarios del grupo** y haga clic en el botón **Agregar**.

   Se abre una ventana con una lista de usuarios.

4. En la lista, seleccione los usuarios que desea incluir en el grupo.

5. Haga clic en **Aceptar**.

El usuario se añade al grupo y se muestra en la lista de usuarios del grupo.

## Configurar los derechos de acceso a las funciones de la aplicación. Control de acceso basado en roles

Kaspersky Security Center proporciona funciones para el acceso basado en roles a las funciones de Kaspersky Security Center y a las de las aplicaciones de Kaspersky administradas.

Puede configurar los derechos de acceso a las funciones de la aplicación para los usuarios de Kaspersky Security Center de una de las siguientes formas:

- Configure los derechos de cada usuario o grupo de usuarios individualmente;
- Cree roles de usuarios estándares con un conjunto predefinido de derechos y asignar esos roles a los usuarios en función del ámbito de sus actividades.

Un *rol de usuario* (también denominado rol) es un conjunto predefinido de derechos de acceso a las funciones de Kaspersky Security Center o de las aplicaciones de Kaspersky administradas. Un rol se puede asignar a un usuario o a un grupo de usuarios.

Aplicar roles de usuario es una manera de simplificar y agilizar la tarea rutinaria de configurar derechos de acceso a las funciones de la aplicación. Cada rol tiene asignados permisos de acceso que responden a las tareas y obligaciones con las que deben cumplir los usuarios.

Los roles de usuario pueden llevar nombres que identifiquen sus propósitos. Puede crear un número ilimitado de roles en la aplicación.

Puede utilizar roles de usuario predefinidos, que vienen configurados con un conjunto de derechos, o puede crear roles nuevos y configurar los derechos necesarios por su cuenta.

## Derechos de acceso a las funciones de la aplicación

En la siguiente tabla, se muestran las funciones de Kaspersky Security Center con los derechos de acceso para administrar las tareas, los informes y las configuraciones asociados y para realizar las acciones del usuario asociadas.

Para realizar las acciones de usuario que se detallan en la tabla, el usuario debe tener el derecho indicado junto a la acción.

Los derechos **Leer**, **Modificar** y **Ejecutar** son aplicables a cualquier tarea, informe o configuración. Además de estos derechos, un usuario debe tener el derecho **Realizar operaciones en selecciones de dispositivos** para administrar tareas, informes o configuraciones en selecciones de dispositivos.

Todas las tareas, informes, configuraciones y paquetes de instalación que faltan en la tabla pertenecen al área funcional de **Características generales: Funcionalidad básica**.

| Área funcional | Derecho | Acción del usuario: derecho necesario para realizar la acción | Tarea | Informe | Otro |
|---|---|---|---|---|---|
| **Características generales: Gestión de grupos de administración** | **Modificar** | • Agregar un dispositivo a un grupo de administración: **Modificar**<br>• Eliminar un dispositivo de un grupo de administración: **Modificar**<br>• Agregar un grupo de administración a otro grupo de administración: **Modificar**<br>• Eliminar un grupo de administración de otro grupo de administración: **Modificar** | Ninguno | N/C | N/C |
| **Características generales: Acceder a objetos sin importar sus ACL** | **Leer** | Obtener acceso Leer a todos los objetos: **Leer** | Ninguno | N/C | N/C |

| Área funcional | Derecho | Acción del usuario: derecho necesario para realizar la acción | Tarea | Informe | Otro |
|---|---|---|---|---|---|
| **Características generales: Funcionalidad básica** | • **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Realizar operaciones en selecciones de dispositivos** | • Reglas de movimiento de dispositivos (crear, modificar o eliminar) para el Servidor virtual: **Modificar**, **Realizar operaciones en selecciones de dispositivos**<br>• Obtener certificado personalizado del protocolo móvil (LWNGT): **Leer**<br>• Establecer certificado personalizado del protocolo móvil (LWNGT): **Modificar**<br>• Obtener la lista de redes definidas por NLA: **Leer**<br>• Agregar, modificar o eliminar la lista de redes definidas por NLA: **Modificar**<br>• Ver la lista de control de acceso de los grupos: **Leer**<br>• Ver el registro de eventos de Kaspersky: **Leer**<br>• Ver la clave de recuperación para restaurar el acceso a un disco duro cifrado con BitLocker: **Ejecutar** | • "Descargar actualizaciones en el repositorio del Servidor de administración"<br>• "Entregar informes"<br>• "Distribuir paquete de instalación"<br>• "Instalar aplicación en Servidores de administración secundarios de forma remota" | • "Informe del estado de la protección"<br>• "Informe de amenazas"<br>• "Informe de los dispositivos más infectados"<br>• "Informe sobre el estado de las bases de datos antivirus"<br>• "Informe de errores"<br>• "Informe de ataques de red"<br>• "Informe conciso sobre las aplicaciones instaladas para la protección de sistemas de correo"<br>• "Informe conciso sobre las aplicaciones instaladas para la defensa del perímetro"<br>• "Informe conciso sobre los tipos de aplicaciones instaladas"<br>• "Informe sobre usuarios de dispositivos infectados"<br>• "Informe sobre incidentes"<br>• "Informe de eventos"<br>• "Informe de actividad de puntos de distribución"<br>• "Informe sobre los Servidores de administración secundarios"<br>• "Informe sobre los eventos de Control de dispositivos"<br>• "Informe de vulnerabilidades"<br>• "Informe sobre aplicaciones prohibidas"<br>• "Informe de Control web"<br>• "Informe sobre el estado de cifrado de los dispositivos administrados" | Ninguno |

| Área funcional | Derecho | Acción del usuario: derecho necesario para realizar la acción | Tarea | Informe | Otro |
|---|---|---|---|---|---|
| | | | | • "Informe sobre el estado de cifrado de los dispositivos de almacenamiento masivo"<br>• "Informe sobre los errores de cifrado de archivos"<br>• "Informe sobre el bloqueo de acceso a los archivos cifrados"<br>• "Informe sobre derechos de acceso a los dispositivos cifrados"<br>• "Informe sobre permisos de usuario vigentes"<br>• "Informe sobre derechos" | |
| **Características generales: Objetos eliminados** | • **Leer**<br>• **Modificar** | • Ver objetos eliminados en la Papelera de reciclaje: **Leer**<br>• Eliminar objetos de la Papelera de reciclaje: **Modificar** | Ninguno | N/C | N/C |
| **Características generales: Procesamiento de eventos** | • **Eliminar eventos**<br>• **Editar configuración de notificación de eventos**<br>• **Editar la configuración de registro de eventos**<br>• **Modificar** | • Cambiar los ajustes de registro de eventos: **Editar la configuración de registro de eventos**<br>• Cambiar la configuración de notificaciones de eventos: **Editar configuración de notificación de eventos**<br>• Eliminar eventos: **Eliminar eventos** | Ninguno | N/C | Configuración:<br>• Configuración de brotes de virus: número de detecciones de virus necesarias para crear un evento de brote de virus<br>• Configuración de brotes de virus: período sobre el que se evalúan las detecciones de virus<br>• Cantidad máxima de eventos almacenados en la base de datos<br>• Período por el que se almacenan los eventos de los dispositivos eliminados |

| Área funcional | Derecho | Acción del usuario: derecho necesario para realizar la acción | Tarea | Informe | Otro |
|---|---|---|---|---|---|
| **Características generales: Operaciones en el Servidor de administración** | • **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Modificar ACL de objeto**<br>• **Realizar operaciones en selecciones de dispositivos** | • Especificar los puertos del Servidor de administración para la conexión del Agente de red: **Modificar**<br>• Especificar los puertos del proxy de activación ejecutado en el Servidor de administración: **Modificar**<br>• Especificar los puertos del proxy de activación para dispositivos móviles ejecutado en el Servidor de administración: **Modificar**<br>• Especificar los puertos del Servidor web para la distribución de paquetes independientes: **Modificar**<br>• Especificar los puertos del Servidor web para la distribución de perfiles de MDM: **Modificar**<br>• Especificar los puertos SSL del Servidor de administración para la conexión a través de Kaspersky Security Center Web Console: **Modificar**<br>• Especificar los puertos del Servidor de administración para la conexión de dispositivos móviles: **Modificar**<br>• Especificar la cantidad máxima de eventos que se pueden almacenar en la base de datos del Servidor de administración: **Modificar**<br>• Especificar la cantidad máxima de eventos que puede enviar el Servidor de administración: **Modificar**<br>• Especificar el período durante el cual puede enviar eventos el Servidor de administración: **Modificar** | • "Copia de seguridad de los datos del Servidor de administración"<br>• "Mantenimiento de bases de datos" | Ninguno | N/C |

| Área funcional | Derecho | Acción del usuario: derecho necesario para realizar la acción | Tarea | Informe | Otro |
|---|---|---|---|---|---|
| **Características generales: Despliegue de la aplicación de Kaspersky** | • **Administrar parches de Kaspersky**<br>• **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Realizar operaciones en selecciones de dispositivos** | Aprobar o rechazar la instalación del parche: **Administrar parches de Kaspersky** | Ninguno | • "Informe sobre el uso de claves de licencia por Servidor de administración virtual"<br>• "Informe de versiones del software de Kaspersky"<br>• "Informe de aplicaciones incompatibles"<br>• "Informe sobre la versión de las actualizaciones para los módulos de software de Kaspersky"<br>• "Informe del despliegue de la protección" | Paquete de instalación: "Kaspersky" |
| **Características generales: Administración de claves de licencia** | • **Exportar archivo de clave**<br>• **Modificar** | • Exportar un archivo de clave: **Exportar archivo de clave**<br>• Modificar la configuración de la clave de licencia del Servidor de administración: **Modificar** | Ninguno | N/C | N/C |
| **Características generales: Administración de informes controlada** | • **Leer**<br>• **Modificar** | • Crear informes independientemente de sus ACL: **Modificar**<br>• Ejecutar informes independientemente de sus ACL: **Leer** | Ninguno | N/C | N/C |
| **Características generales: Jerarquía de Servidores de administración** | **Configurar la jerarquía de Servidores de administración** | Registrar, actualizar o eliminar Servidores de administración secundarios: **Configurar la jerarquía de Servidores de administración** | Ninguno | N/C | N/C |
| **Características generales: Permisos de usuario** | **Modificar ACL de objeto** | • Cambiar las propiedades de seguridad de cualquier objeto: **Modificar ACL de objeto**<br>• Administrar roles de usuario: **Modificar ACL de objeto**<br>• Administrar usuarios internos: **Modificar ACL de objeto**<br>• Administrar grupos de seguridad: **Modificar ACL de objeto**<br>• Administrar alias: **Modificar ACL de objeto** | Ninguno | N/C | N/C |

| Área funcional | Derecho | Acción del usuario: derecho necesario para realizar la acción | Tarea | Informe | Otro |
|---|---|---|---|---|---|
| **Características generales: Servidores de administración virtuales** | • **Administrar Servidores de administración virtuales**<br>• **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Realizar operaciones en selecciones de dispositivos** | • Obtener la lista de Servidores de administración virtuales: **Leer**<br>• Obtener información sobre el Servidor de administración virtual: **Leer**<br>• Crear, actualizar o eliminar un Servidor de administración virtual: **Administrar Servidores de administración virtuales**<br>• Mover un Servidor de administración virtual a otro grupo: **Administrar Servidores de administración virtuales**<br>• Definir los permisos de un Servidor de administración virtual: **Administrar Servidores de administración virtuales** | Ninguno | "Informe sobre los resultados de la instalación de actualizaciones de software de terceros" | Ninguno |
| **Características generales: Administración de claves de cifrado** | • **Leer**<br>• **Modificar** | • Exportar las claves de cifrado: **Leer**<br>• Importar las claves de cifrado: **Modificar** | Ninguno | N/C | N/C |

| Área funcional | Derecho | Acción del usuario: derecho necesario para realizar la acción | Tarea | Informe | Otro |
|---|---|---|---|---|---|
| **Administración de dispositivos móviles: General** | • **Conectar nuevos dispositivos**<br>• **Enviar únicamente comandos de información a dispositivos móviles**<br>• **Enviar comandos a dispositivos móviles**<br>• **Administrar certificados**<br>• **Leer**<br>• **Modificar** | • Obtener datos de restauración del servicio de administración de claves: **Leer**<br>• Eliminar certificados de usuario: **Administrar certificados**<br>• Obtener la parte pública de un certificado de usuario: **Leer**<br>• Comprobar si la infraestructura de claves públicas está habilitada: **Leer**<br>• Comprobar la cuenta de la infraestructura de claves públicas: **Leer**<br>• Obtener plantillas de la infraestructura de claves públicas: **Leer**<br>• Obtener plantillas de la infraestructura de claves públicas mediante un certificado de uso extendido de clave: **Leer**<br>• Comprobar si el certificado de la infraestructura de claves públicas fue revocado: **Leer**<br>• Actualizar la configuración de emisión de certificados de usuario: **Administrar certificados**<br>• Obtener la configuración de emisión de certificados de usuario: **Leer**<br>• Obtener paquetes por nombre y versión de aplicación: **Leer**<br>• Definir o cancelar un certificado de usuario: **Administrar certificados**<br>• Renovar un certificado de usuario: **Administrar certificados**<br>• Definir una etiqueta para un certificado de usuario: **Administrar certificados**<br>• Ejecutar la generación del paquete de instalación de MDM; cancelar la generación del paquete de instalación de MDM: | Ninguno | N/C | N/C |

| Área funcional | Derecho | Acción del usuario: derecho necesario para realizar la acción | Tarea | Informe | Otro |
|---|---|---|---|---|---|
| | | **Conectar nuevos dispositivos** | | | |
| **Administración de sistemas: Conectividad** | • **Iniciar sesiones RDP**<br>• **Conexión a sesiones de RDP existentes**<br>• **Iniciar la tunelización**<br>• **Guardar archivos de los dispositivos en la estación de trabajo del administrador**<br>• **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Realizar operaciones en selecciones de dispositivos** | • Crear sesión de escritorio compartido: **Iniciar sesiones RDP**<br>• Crear una sesión de RDP: **Conexión a sesiones de RDP existentes**<br>• Crear un túnel: **Iniciar la tunelización**<br>• Guardar la lista de red de contenido: **Guardar archivos de los dispositivos en la estación de trabajo del administrador** | Ninguno | "Informe sobre los usuarios de los dispositivos" | Ninguno |
| **Administración de sistemas: Inventario de hardware** | • **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Realizar operaciones en selecciones de dispositivos** | • Obtener o exportar un objeto del inventario de hardware: **Leer**<br>• Agregar, definir o eliminar un objeto del inventario de hardware: **Modificar** | Ninguno | • "Informe sobre el registro de hardware"<br>• "Informe sobre los cambios en la configuración"<br>• "Informe de hardware" | Ninguno |
| **Administración de sistemas: Control de acceso a la red** | • **Leer**<br>• **Modificar** | • Ver la configuración de CISCO: **Leer**<br>• Cambiar la configuración de CISCO: **Modificar** | Ninguno | N/C | N/C |
| **Administración de sistemas: Despliegue de sistemas operativos** | • **Desplegar servidores PXE**<br>• **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Realizar operaciones en selecciones de dispositivos** | • Desplegar servidores PXE: **Desplegar servidores PXE**<br>• Ver una lista de servidores PXE: **Leer**<br>• Iniciar o detener el proceso de instalación en clientes PXE: **Ejecutar**<br>• Administrar controladores para WinPE e imágenes de sistema operativo: **Modificar** | "Crear un paquete de instalación con la imagen del SO de un dispositivo de referencia" | Ninguno | Paquete de instalación: "Imagen del SO" |

| Área funcional | Derecho | Acción del usuario: derecho necesario para realizar la acción | Tarea | Informe | Otro |
|---|---|---|---|---|---|
| **Administración de sistemas: Administración de vulnerabilidades y parches** | • **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Realizar operaciones en selecciones de dispositivos** | • Ver propiedades de parches de terceros: **Leer**<br>• Cambiar las propiedades de parches de terceros: **Modificar** | • "Sincronización con Windows Update"<br>• "Instalar actualizaciones de Windows Update"<br>• "Reparar vulnerabilidades"<br>• "Instalar actualizaciones requeridas y reparar vulnerabilidades" | "Informe de actualizaciones de software" | Ninguno |
| **Administración de sistemas: Instalación remota** | • **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Realizar operaciones en selecciones de dispositivos** | • Ver las propiedades de un paquete de instalación de una aplicación de terceros (con Administración de vulnerabilidades y parches habilitada): **Leer**<br>• Cambiar las propiedades de un paquete de instalación de una aplicación de terceros (con Administración de vulnerabilidades y parches habilitada): **Modificar** | Ninguno | N/C | Paquetes de instalación:<br>• "Aplicación personalizada"<br>• "Paquete VAPM" |
| **Administración de sistemas: Inventario de software** | • **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Realizar operaciones en selecciones de dispositivos** | Ninguno | N/C | • "Informe sobre aplicaciones instaladas"<br>• "Informe del historial del registro de aplicaciones"<br>• "Informe sobre el estado de los grupos de aplicaciones con licencia"<br>• "Informe sobre claves de licencia de software de terceros" | Ninguno |

## Roles de usuario predefinidos

Los roles de usuario asignados a los usuarios de Kaspersky Security Center les brindan los conjuntos de derechos que necesitan para acceder a las funciones de la aplicación.

A los usuarios creados en un Servidor virtual no se les puede asignar una función en el Servidor de administración.

Puede utilizar roles de usuario predefinidos, que vienen configurados con un conjunto de derechos, o puede crear roles nuevos. En este caso, debe establecer el alcance del rol y asignar los derechos de acceso a las funciones de Kaspersky Security Center por su cuenta. Algunos de los roles predefinidos de Kaspersky Security Center se pueden asociar con puestos de trabajo específicos; es el caso, por ejemplo, de los roles **Auditor**, **Supervisor** y **Director de seguridad**, que han estado disponibles en Kaspersky Security Center desde la versión 11. Los derechos de acceso de estos roles están preconfigurados para facilitar las obligaciones y las tareas típicas de los puestos asociados. En la siguiente tabla, se muestra cómo estos roles pueden vincularse a puestos de trabajo específicos.

Ejemplos de roles para puestos de trabajo específicos

| Rol | Comentario |
|---|---|
| Auditor | Permite todas las operaciones de visualización y ejecución de las tareas creadas en selecciones de dispositivos conectados al Servidor de administración a través del Agente de red con derechos de administrador local (raíz para Linux).<br><br>Recomendamos asignar esta función con cuidado y a un grupo limitado de usuarios que la necesiten para desempeñar sus funciones oficiales. |
| Supervisor | Permite realizar cualquier operación de visualización; no permite realizar otras operaciones. Puede asignar este rol a un oficial de seguridad y a otras personas que tengan a su cargo la seguridad de TI de la organización. |
| Oficial de seguridad | Permite realizar cualquier operación de visualización y permite administrar los informes; también otorga permisos limitados en el área **Administración de sistemas**: **Conectividad**. Puede asignar este rol al responsable de la seguridad de TI de su organización. |

En la siguiente tabla, se muestran los derechos de acceso asignados a cada rol de usuario predefinido.

Derechos de acceso de los roles de usuario predefinidos

| Rol | Descripción |
|---|---|
| Administrador del Servidor de administración | Permite todas las operaciones en las siguientes áreas funcionales:<br>• **Características generales**:<br>  • **Funcionalidad básica**<br>  • **Procesamiento de eventos**<br>  • **Jerarquía de Servidores de administración**<br>  • **Servidores de administración virtuales**<br>• **Administración de sistemas**:<br>  • **Conectividad**<br>  • **Inventario de hardware**<br>  • **Inventario de software**<br><br>Otorga los derechos **Leer** y **Escribir** en el área funcional **Características generales: Administración de claves de cifrado**. |
| Operador del Servidor de administración | Otorga los derechos **Leer** y **Ejecutar** en las siguientes áreas funcionales:<br>• **Características generales**:<br>  • **Funcionalidad básica**<br>  • **Servidores de administración virtuales**<br>• **Administración de sistemas**:<br>  • **Conectividad**<br>  • **Inventario de hardware**<br>  • **Inventario de software** |

| Rol | Descripción |
| --- | --- |
| Auditor | Permite todas las operaciones en todas las áreas funcionales, en **Características generales**:<br>• **Acceder a objetos sin importar sus ACL**<br>• **Objetos eliminados**<br>• **Administración de informes controlada**<br>Puede asignar este rol a la persona que realiza la auditoría de su organización. |
| Administrador de instalación | Permite todas las operaciones en las siguientes áreas funcionales:<br>• **Características generales**:<br>  • **Funcionalidad básica**<br>  • **Despliegue del software de Kaspersky**<br>  • **Administración de claves de licencia**<br>• **Administración de sistemas**:<br>  • **Despliegue del sistema operativo**<br>  • **Administración de vulnerabilidades y parches**<br>  • **Instalación remota**<br>  • **Inventario de software**<br>Otorga los derechos **Leer** y **Ejecutar** en el área funcional **Características generales: Servidores de administración virtuales**. |
| Operador de instalación | Otorga los derechos **Leer** y **Ejecutar** en las siguientes áreas funcionales:<br>• **Características generales**:<br>  • **Funcionalidad básica**<br>  • **Despliegue del software de Kaspersky** (también otorga el derecho **Administrar parches de Kaspersky** en esta área)<br>  • **Servidores de administración virtuales**<br>• **Administración de sistemas**:<br>  • **Despliegue del sistema operativo**<br>  • **Administración de vulnerabilidades y parches**<br>  • **Instalación remota**<br>  • **Inventario de software** |
| Administrador de Kaspersky Endpoint Security | Permite todas las operaciones en las siguientes áreas funcionales:<br>• **Características generales: funcionalidad básica**<br>• Área de Kaspersky Endpoint Security (se incluyen todas las funciones)<br>Otorga los derechos **Leer** y **Escribir** en el área funcional **Características generales: Administración de claves de cifrado**. |
| Operador de Kaspersky Endpoint Security | Otorga los derechos **Leer** y **Ejecutar** en las siguientes áreas funcionales:<br>• **Características generales: funcionalidad básica**<br>• Área de Kaspersky Endpoint Security (se incluyen todas las funciones) |
| Administrador principal | Permite todas las operaciones en todas las áreas funcionales, *excepto* en las siguientes áreas, en **Características generales**:<br>• **Acceder a objetos sin importar sus ACL**<br>• **Administración de informes forzados**<br>Otorga los derechos **Leer** y **Escribir** en el área funcional **Características generales: Administración de claves de cifrado**. |

| Rol | Descripción |
| --- | --- |
| Operador principal | Otorga los derechos **Leer** y **Ejecutar** (cuando corresponde) en las siguientes áreas funcionales:<br>• **Características generales**:<br>  • **Funcionalidad básica**<br>  • **Objetos eliminados**<br>  • **Operaciones en el Servidor de administración**<br>  • **Despliegue de la aplicación de Kaspersky**<br>  • **Servidores de administración virtuales**<br>• **Administración de dispositivos móviles: General**<br>• **Administración de sistemas** (se incluyen todas las funciones)<br>• Área de Kaspersky Endpoint Security (se incluyen todas las funciones) |
| Administrador de Administración de dispositivos móviles | Permite todas las operaciones en las siguientes áreas funcionales:<br>• **Características generales: funcionalidad básica**<br>• **Administración de dispositivos móviles: General** |
| Operador de Administración de dispositivos móviles | Otorga los derechos **Leer** y **Ejecutar** en el área funcional **Características generales**: **Funcionalidad básica**.<br>Otorga los derechos **Leer** y **Enviar únicamente comandos de información a dispositivos móviles** en **Administración de dispositivos móviles**: **General** área funcional: |
| Director de seguridad | Permite todas las operaciones en las siguientes áreas funcionales, en **Características generales**:<br>• **Acceder a objetos sin importar sus ACL**<br>• **Administración de informes controlada**<br>Otorga los derechos **Leer**, **Escribir**, **Ejecutar**, **Guardar archivos de los dispositivos en la estación de trabajo del administrador** y **Realizar operaciones en selecciones de dispositivos** en el área funcional **Administración de sistemas: Conectividad**.<br>Puede asignar este rol al responsable de la seguridad de TI de su organización. |
| Usuario de Self Service Portal | Permite todas las operaciones en el área funcional **Administración de dispositivos móviles: Self Service Portal**. Esta función no es compatible con Kaspersky Security Center 11 ni versiones posteriores. |
| Supervisor | Otorga el derecho **Leer** en las áreas funcionales **Características generales**: **Acceder a objetos sin importar sus ACL** y **Características generales**: **Administración de informes controlada**.<br>Puede asignar este rol a un Director de seguridad y a otras personas que tengan a su cargo la seguridad de TI de la organización. |
| Administrador de Administración de vulnerabilidades y parches | Permite todas las operaciones en las áreas funcionales **Características generales**: **Funcionalidad básica** y **Administración de sistemas** (se incluyen todas las funciones). |
| Operador de Administración de vulnerabilidades y parches | Otorga los derechos **Leer** y **Ejecutar** (cuando corresponde) en las áreas funcionales **Características generales**: **Funcionalidad básica** y **Administración de sistemas** (se incluyen todas las funciones). |

## Agregar un rol de usuario

*Para agregar un rol de usuario:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.

3. En la ventana Propiedades del Servidor de administración, en el panel **Secciones** seleccione **Roles de usuario** y haga clic en el botón **Agregar**.

   La sección **Roles de usuario** está disponible si la opción **Mostrar secciones de configuración de seguridad** está habilitada.

4. En la ventana de propiedades del **Rol nuevo**, configure el rol:

   - En las **Secciones**, seleccione **General** y especifique el nombre del rol.

     El nombre de un rol no puede contener más de 100 caracteres.

   - Seleccione la sección **Derechos**, y configure el conjunto de permisos seleccionando las casillas **Permitir** y **Denegar** que se encuentran junto a las características de la aplicación.

   Si está operando en el Servidor de administración principal, puede habilitar la opción **Retransmitir la lista de roles a los Servidores de administración secundarios**.

5. Haga clic en **Aceptar**.

Se agrega el rol.

Los roles de usuarios que se han creado para el Servidor de administración se muestran en la ventana de propiedades del Servidor de administración, en la sección **Roles de usuario**. Puede modificar y eliminar roles de usuarios, así como asignar roles a grupos de seguridad o usuarios seleccionados.

## Asignación de un rol a un usuario o a un grupo de seguridad

*Para asignar un rol a un usuario o grupo de usuarios:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
3. En la ventana de propiedades del Servidor de administración, seleccione la sección **Seguridad**.

   La sección **Seguridad** está disponible si la casilla **Mostrar secciones de configuración de seguridad** está seleccionada en la ventana de configuración de la interfaz.

4. En el campo **Nombres de grupos o usuarios**, seleccione un usuario o grupo de usuarios a los que se les debe asignar un rol.

   Si el usuario o el grupo no están incluidos en el campo, puede agregarlos haciendo clic en el botón **Agregar**.

   Cuando agrega un usuario haciendo clic en el botón **Agregar**, puede seleccionar el tipo de autenticación del usuario (Microsoft Windows o Kaspersky Security Center). La autenticación de Kaspersky Security Center se usa para seleccionar las cuentas de los usuarios internos que se usan para trabajar con los Servidores de administración virtuales.

5. Abra la pestaña **Roles** y haga clic en el botón **Agregar**.

   Se abre la ventana **Roles de usuarios**. En esta ventana se muestran los roles de usuarios que se han creado.

6. En la ventana **Roles de usuarios**, seleccione un rol para el grupo de seguridad.

7. Haga clic en **Aceptar**.

El rol con un conjunto de permisos para trabajar en el Servidor de administración se asigna al usuario o grupo de seguridad. Los roles que se han asignado se muestran en la pestaña **Roles** en la sección **Seguridad** de la ventana de propiedades del Servidor de administración.

## Asignación de permisos a usuarios y grupos

Puede otorgar a los usuarios y a los grupos permisos para usar diferentes funciones del Servidor de administración y de los programas de Kaspersky para los cuales tiene complementos de administración, por ejemplo, Kaspersky Endpoint Security para Windows.

*Para asignar permisos a un usuario o un grupo de usuarios:*

1. En el árbol de la consola, realice una de las siguientes acciones:

   - Expanda el nodo del **Servidor de administración** y seleccione la subcarpeta con el nombre del Servidor de administración requerido.

   - Seleccione el grupo de administración.

2. Seleccione **Propiedades** en el menú contextual del Servidor de administración o grupo de administración.

3. En la ventana de propiedades del Servidor de administración (o la ventana de propiedades del grupo de administración) que se abre, en el panel **Secciones** de la izquierda, seleccione **Seguridad**.

   La sección **Seguridad** está disponible si la casilla **Mostrar secciones de configuración de seguridad** está seleccionada en la ventana de configuración de la interfaz.

4. En la sección **Seguridad**, en la lista **Nombres de grupos o usuarios**, seleccione un usuario o un grupo.

5. En la lista de permisos en la parte inferior del espacio de trabajo, en la pestaña **Derechos** configurar el conjunto de derechos para el usuario o grupo:

   a. Haga clic en los signos más (+) para expandir los nodos en la lista y obtener acceso a los permisos.

   b. Seleccione las casillas de verificación **Permitir** y **Denegar** junto a los permisos que desee.

      *Ejemplo 1:* Expanda los objetos de **Acceder a objetos sin importar sus ACL** o su nodo **Objetos eliminados**, y seleccione **Leer**.

      *Ejemplo 2:* Amplíe el nodo de funcionalidad **Básico** y seleccione **Modificar**.

6. Cuando haya configurado el conjunto de derechos, haga clic en **Aplicar**.

Se configurará el conjunto de derechos para el usuario o grupo de usuarios.

Los permisos del Servidor de administración (o el grupo de administración) se dividen en las siguientes áreas:

- Características generales:
  - Gestión de grupos de administración
  - Acceder a objetos sin importar sus ACL
  - Funcionalidad básica
  - Objetos eliminados
  - Procesamiento de eventos
  - Operaciones en el Servidor de administración (solo en la ventana de propiedades del Servidor de administración)
  - Desplegar aplicaciones de Kaspersky
  - Administración de claves de licencia
  - Administración de informes controlada
  - Jerarquía de servidores
  - Derechos del usuario
  - Servidores de administración virtuales
- Administración de dispositivos móviles:
  - General
- Administración de sistemas:
  - Conectividad
  - Inventario de hardware
  - Control de acceso a la red
  - Despliegue de sistemas operativos
  - Administrar vulnerabilidades y parches
  - Instalación remota
  - Inventario de software

Si no se selecciona **Permitir** ni **Denegar** para un permiso, el permiso se considera *indefinido*: se deniega hasta que se deniegue o permita explícitamente al usuario.

Los derechos de un usuario son la suma de lo siguiente:

- los propios derechos del usuario
- los derechos de todos los roles asignados al usuario
- los derechos de todo el grupo de seguridad al que pertenece el usuario
- los derechos de todos los roles asignados a los grupos de seguridad a los que pertenece el usuario

Si al menos uno de estos conjuntos de derechos tiene **Denegar** para un permiso, al usuario se le niega este permiso, incluso si otros conjuntos lo permiten o lo dejan sin definir.

## Propagación de roles de usuario a Servidores de administración secundarios

De forma predeterminada, las listas de funciones del usuario de los Servidores de administración principal y secundario son independientes. Puede configurar la aplicación para propagar automáticamente las funciones de usuario creadas en el Servidor de administración principal a todos los Servidores de administración secundarios. Las funciones de usuario también pueden propagarse desde un Servidor de administración secundario a sus propios Servidores de administración secundarios.

*Para propagar funciones de usuario desde el Servidor de administración principal a los Servidores de administración secundarios:*

1. Abra la ventana principal de la aplicación.
2. Realice una de las siguientes acciones:
   - En el árbol de la consola, haga clic con el botón derecho en el nombre del Servidor de administración y seleccione **Propiedades** en el menú contextual.
   - Si tiene una directiva del Servidor de administración activa, en el espacio de trabajo de la carpeta **Directivas**, haga clic en esta directiva con el botón derecho del ratón y seleccione **Propiedades** en el menú contextual.
3. En la ventana de propiedades del Servidor de administración o en la ventana de la configuración de la directiva, en el panel **Secciones** seleccione **Funciones de usuario**.

   La sección **Roles de usuario** está disponible si la opción **Mostrar secciones de configuración de seguridad** está habilitada.

4. Habilite la opción **Propagar la lista de roles a los Servidores de administración secundarios**.
5. Haga clic en **Aceptar**.

   La aplicación copia las funciones de usuario del Servidor de administración principal a los Servidores de administración secundarios.

Cuando la opción **Propagar la lista de roles a los Servidores de administración secundarios** está habilitada y las funciones de usuario se propagan, no se pueden editar ni eliminar en los Servidores de administración secundarios. Cuando crea una nueva función o edita una existente en el Servidor de administración principal, los cambios se copian automáticamente en los Servidores de administración secundarios. Cuando elimina una función de usuario en el Servidor de administración principal, esta función permanece en los Servidores de administración secundarios posteriormente, pero se puede editar o eliminar.

Las funciones que se propagan al Servidor de administración secundario desde el Servidor principal se muestran con el ícono de candado (🔒). No puede modificar estas funciones en el Servidor de administración secundario.

Si crea una función en el Servidor de administración principal y hay una función con el mismo nombre en su Servidor de administración secundarios, el nuevo rol se copia al Servidor de administración secundario con el índice agregado a su nombre, por ejemplo, ~~ 1, ~~ 2 (el índice puede ser aleatorio).

Si deshabilita la opción **Propagar la lista de roles a los Servidores de administración secundarios**, todas las funciones de usuario permanecen en los Servidores de administración secundarios, pero se vuelven independientes de las del Servidor de administración principal. Después de volverse independientes, las funciones de usuario de los Servidores de administración secundarios se pueden editar o eliminar.

## Asignar al usuario como propietario del dispositivo

Puede nombrar al usuario como propietario del dispositivo para asignar el dispositivo a ese usuario. Si debe realizar algunas acciones en el dispositivo (por ejemplo, actualizar el hardware), el administrador puede notificar al propietario del dispositivo para que autorice dichas acciones.

*Para asignar a un usuario como propietario de un dispositivo:*

1. En el árbol de consola, seleccione la carpeta **Dispositivos administrados**.
2. En el espacio de trabajo de la carpeta, en la pestaña **Dispositivos**, seleccione el dispositivo para el que desea asignar un propietario.
3. En el menú contextual del dispositivo, seleccione **Propiedades**.
4. En la ventana de propiedades del dispositivo, seleccione **Información del sistema** → **Sesiones**.
5. Haga clic en el botón **Asignar** al lado del campo **Propietario del dispositivo**.
6. En la ventana **Selección de usuario**, seleccione al usuario que desea asignar como propietario del dispositivo y haga clic en el botón **Aceptar**.
7. Haga clic en **Aceptar**.

El propietario del dispositivo se asignó. De manera predeterminada, el campo **Propietario del dispositivo** incluye un valor de Active Directory y se actualiza durante cada sondeo de Active Directory. Puede ver la lista de propietarios de dispositivos en el **Informe sobre propietarios de dispositivos**. Puede crear un informe usando el Asistente de nueva plantilla de informe.

## Enviar mensajes a los usuarios

*Para enviar un mensaje por correo electrónico a un usuario:*

1. En el árbol de consola, en la carpeta **Cuentas de usuario**, seleccione un usuario.

   De manera predeterminada, la carpeta **Cuentas de usuario** es una subcarpeta de la carpeta **Avanzado**.
2. En el menú contextual del usuario, seleccione **Notificar por correo electrónico**.
3. Complete los campos correspondientes en la ventana **Enviar mensaje a usuario** y haga clic en el botón **Aceptar**.

El mensaje se enviará a la dirección de correo electrónico que se especificó en las propiedades del usuario.

*Para enviar un mensaje de texto a un usuario:*

1. En el árbol de consola, en la carpeta **Cuentas de usuario**, seleccione un usuario.
2. En el menú contextual del usuario, seleccione **Enviar un SMS**.
3. Complete los campos correspondientes en la ventana **Texto de SMS** y haga clic en el botón **Aceptar**.

El mensaje se enviará al dispositivo móvil con el número que se especificó en las propiedades del usuario.

## Ver la lista de dispositivos móviles de los usuarios

*Para ver la lista de dispositivos móviles de un usuario:*

1. En el árbol de consola, en la carpeta **Cuentas de usuario**, seleccione un usuario.

   De manera predeterminada, la carpeta **Cuentas de usuario** es una subcarpeta de la carpeta **Avanzado**.
2. En el menú contextual de la cuenta de usuario, seleccione **Propiedades**.
3. En la ventana de propiedades de la cuenta de usuario, seleccione la sección **Dispositivos móviles**.

En la sección **Dispositivos móviles**, puede ver la lista de dispositivos móviles del usuario y la información sobre cada uno de ellos. Puede hacer clic en el botón **Exportar a archivo** para guardar la lista de dispositivos móviles en un archivo.

## Instalar un certificado para un usuario

Puede instalar tres tipos de certificados para un usuario:

- Certificado compartido, que es necesario para identificar el dispositivo móvil del usuario.
- Certificado de correo, que es necesario para configurar el correo corporativo en el dispositivo móvil del usuario.
- Certificado de VPN, que es necesario para configurar la red privada virtual en el dispositivo móvil del usuario.

*Para emitir un certificado a un usuario y luego instalarlo:*

1. En el árbol de consola, abra la carpeta **Cuentas de usuario** y seleccione una cuenta de usuario.

   De manera predeterminada, la carpeta **Cuentas de usuario** es una subcarpeta de la carpeta **Avanzado**.
2. En el menú contextual de la cuenta de usuario, seleccione **Instalar certificado**.

Se inicia el Asistente de instalación de certificados. Siga las instrucciones del asistente.

Después de que haya finalizado el Asistente de instalación de certificados, el certificado se creará e instalará para el usuario. Puede ver la lista de certificados de usuario instalados y exportarlos a un archivo.

## Ver la lista de certificados emitidos para un usuario

*Para ver una lista de todos los certificados emitidos a un usuario:*

1. En el árbol de consola, en la carpeta **Cuentas de usuario**, seleccione un usuario.

   De manera predeterminada, la carpeta **Cuentas de usuario** es una subcarpeta de la carpeta **Avanzado**.

2. En el menú contextual de la cuenta de usuario, seleccione **Propiedades**.

3. En la ventana de propiedades de la cuenta de usuario, seleccione la sección **Certificados**.

En la sección **Certificados** puede ver la lista de los certificados del usuario y la información sobre cada uno de ellos. Puede hacer clic en el botón **Exportar a archivo** para guardar la lista de certificados en un archivo.

## Acerca del administrador del Servidor de administración virtual

Un administrador de la red empresarial administrada a través de un Servidor de administración virtual inicia la Kaspersky Security Center Web Console en la cuenta de usuario especificada en esta ventana para ver los detalles de la protección antivirus.

Si es necesario, pueden crearse varias cuentas de administrador en un Servidor virtual.

A los usuarios creados en un Servidor virtual no se les puede asignar una función en el Servidor de administración.

El administrador de un Servidor de administración virtual es un usuario interno de Kaspersky Security Center. No se transfiere ningún dato sobre estos usuarios internos al sistema operativo. Kaspersky Security Center se encarga de autenticar a los usuarios internos.

# Instalación remota de sistemas operativos y aplicaciones

Kaspersky Security Center permite crear imágenes de los sistemas operativos e instalarlas de forma remota en los dispositivos cliente de la red. También permite realizar instalaciones remotas de aplicaciones de Kaspersky o de otros proveedores.

Para crear imágenes de sistemas operativos, instale las herramientas de despliegue de Windows ADK y el complemento de Windows PE para Windows ADK en el Servidor de administración. Puede crear una imagen de cualquier versión del sistema operativo Windows que cumpla con los requisitos de Kaspersky Security Center.

Kaspersky Security Center no es compatible con las versiones de 64 bits de Windows ADK y Windows PE.

## Capturar imágenes de sistemas operativos

Kaspersky Security Center puede capturar imágenes de los sistemas operativos de los dispositivos y transferir esas imágenes al Servidor de administración. Estas imágenes de los sistemas operativos se almacenan en el Servidor de administración, en una carpeta dedicada. Se captura y crea la imagen del sistema operativo de un dispositivo de referencia mediante una tarea de creación del paquete de instalación.

La funcionalidad de la captura de imágenes de los sistemas operativos tiene las siguientes características:

- No se puede capturar una imagen de un sistema operativo en un dispositivo en el que está instalado el Servidor de administración.
- Mientras se captura una imagen del sistema operativo, la utilidad sysprep.exe restablece la configuración del dispositivo de referencia. Si desea restaurar la configuración del dispositivo de referencia, seleccione la casilla **Crear una copia de seguridad del estado del dispositivo** en el Asistente para crear una tarea de captura de imagen de SO.
- El proceso de captura de imágenes posibilita el reinicio del dispositivo de referencia.

## Instalación remota de imágenes de sistemas operativos en dispositivos nuevos

Puede usar las imágenes recibidas para instalarlas en dispositivos de la red que aún no cuenten con un sistema operativo. En este caso se utiliza una tecnología denominada Preboot eXecution Environment (PXE). Debe seleccionar un dispositivo en red para utilizar como servidor PXE. Este dispositivo debe reunir los siguientes requisitos:

- El Agente de red debe estar instalado en el dispositivo.
- No debe haber ningún servidor DHCP activo en el dispositivo, ya que el servidor PXE utiliza los mismos puertos que un servidor DHCP.
- El segmento de la red que incluye al dispositivo no debe contener ningún otro servidor PXE.

Deben cumplirse las siguientes condiciones para implementar un sistema operativo:

- Debe haber una tarjeta de red montada en el dispositivo.
- El dispositivo debe estar conectado a la red.
- Debe seleccionarse la opción Inicio de la red en la BIOS al iniciar el dispositivo.

La instalación remota de un sistema operativo se realiza de la siguiente manera:

1. El dispositivo cliente establece una conexión con el servidor PXE durante el proceso de inicio.
2. El dispositivo cliente se inicia en el Entorno de preinstalación de Windows (WinPE).

   Agregar el dispositivo a WinPE puede requerir configuración del conjunto de controladores de WinPE.

3. El dispositivo cliente se registra en el Servidor de administración.

4. El administrador le asigna al dispositivo cliente un paquete de instalación con una imagen del sistema operativo.

   El administrador puede agregar los controladores requeridos al paquete de instalación con la imagen del sistema operativo. El administrador también puede especificar un archivo de configuración con la configuración del sistema operativo (archivo de respuesta) que se debe aplicar durante la instalación.

5. El sistema operativo se instala en el dispositivo cliente.

El administrador puede especificar manualmente las direcciones MAC de los dispositivos cliente que aún no se han conectado y asignarles el paquete de instalación con la imagen del sistema operativo. Cuando los dispositivos cliente seleccionados se conectan al servidor PXE, el sistema operativo se instala automáticamente en esos dispositivos.

### Instalación de una imagen de sistema operativo en dispositivos que ya cuentan con otro sistema operativo

La instalación de imágenes de sistema operativo en dispositivos cliente que ya cuentan con otro sistema operativo se realiza a través de la tarea de instalación remota para dispositivos específicos.

Tenga en cuenta que se realiza una instalación limpia del sistema operativo. Se eliminarán todos los datos.

### Instalación de aplicaciones desarrolladas por Kaspersky y otros proveedores

El administrador puede crear paquetes de instalación de cualquier aplicación, incluso aquellas especificadas por el usuario, e instalar estas aplicaciones en dispositivos cliente mediante la tarea de instalación remota.

## Crear imágenes de sistemas operativos

Las imágenes de sistemas operativos se crean usando la tarea de eliminar la imagen del sistema operativo del dispositivo de referencia.

*Para crear la tarea de generación de imagen del sistema operativo:*

1. En la carpeta **Instalación remota** del árbol de la consola, seleccione la subcarpeta **Paquetes de instalación**.
2. Haga clic en el botón **Crear paquete de instalación** para ejecutar el Asistente de nuevo paquete.
3. En la ventana **Seleccione un tipo de paquete de instalación** del Asistente, haga clic en el botón **Crear un paquete de instalación basado en la imagen del sistema operativo**.
4. Siga las instrucciones del asistente.

   Cuando el Asistente finaliza, se crea una tarea del Servidor de administración denominada **Crear un paquete de instalación basado en la imagen del SO de un dispositivo de referencia**. Puede visualizar la tarea en la carpeta **Tareas**.

Cuando se completa la tarea **Crear un paquete de instalación basado en la imagen del SO de un dispositivo de referencia**, se crea un paquete de instalación que puede usar para instalar el sistema operativo en los dispositivos cliente mediante un servidor PXE o con la tarea de instalación remota. Puede ver el paquete de instalación en la carpeta **Paquetes de instalación**.

# Instalación de imágenes de los sistemas operativos

Kaspersky Security Center le permite distribuir imágenes WIM de sistemas operativos de Windows® de escritorio y basados en el servidor en dispositivos dentro de una red de la organización.

Los métodos siguientes pueden ser usados para recuperar una imagen del sistema operativo que se podría distribuir usando herramientas de Kaspersky Security Center:

- Importar el archivo install.wim incluido en el paquete de distribución de Windows
- Capturar una imagen desde un dispositivo de referencia

La instalación de imágenes de sistema operativo puede realizarse en dos contextos:

- Instalación en un dispositivo "limpio", es decir, uno que no tiene ningún sistema operativo instalado
- Instalación en un dispositivo que tiene Windows instalado

Utilice el entorno de preinstalación de Windows (Windows PE) para capturar e implementar imágenes del sistema operativo. Todos los controladores requeridos para el correcto funcionamiento de todos los dispositivos de destino se deben agregar a WinPE. Por lo general, se deben agregar controladores de las unidades de almacenamiento y del adaptador de red.

Para capturar e instalar las imágenes, se deben cumplir los siguientes requisitos:

- El Kit de instalación automatizada de Windows (WAIK) versión 2.0 o posterior, o Windows ADK con el complemento de Windows PE para Windows ADK debe estar instalado en el Servidor de administración. Si la situación permite la instalación o la captura de imágenes en Windows XP, WAIK se debe instalar.
- Un servidor DHCP debe estar disponible en la red donde se encuentra el dispositivo de destino.
- La carpeta compartida del Servidor de administración debe estar abierta para lectura desde la red donde el dispositivo de destino se localiza. Si la carpeta compartida se ubica en el Servidor de administración, se requiere acceso para la cuenta de KlPxeUser (esta cuenta se crea automáticamente al ejecutar el Instalador del Servidor de administración). Si la carpeta compartida se localiza fuera del Servidor de administración, el acceso se debe conceder a todos los usuarios.

Al seleccionar la imagen del sistema operativo que se debe instalar, el administrador debe especificar explícitamente la arquitectura de la CPU del dispositivo de destino: x86 o x86-64.

# Configurar la dirección del servidor proxy de KSN

De manera predeterminada, el nombre de conexión o la dirección IP del Servidor de administración coincide con la dirección del servidor proxy de KSN. Si cambia el nombre el nombre de conexión o la dirección IP del Servidor de administración, debe especificar la dirección correcta del servidor proxy de KSN para evitar que se pierda la conexión entre los dispositivos host y el KSN.

*Para configurar la dirección del proxy de KSN, siga estos pasos:*

1. En el árbol de la consola, vaya a **Avanzado** → **Instalación remota** → **Paquetes de instalación**.
2. En el menú contextual de **Paquetes de instalación**, seleccione **Propiedades**.

3. En la ventana que se abre, especifique la nueva dirección del proxy de KSN en la pestaña **General**.

4. Haga clic en el botón **Aplicar**.

A partir de ahora, la dirección especificada se utiliza como dirección del proxy de KSN. Le recomendamos que habilite la opción **Usar proxy de KSN** para optimizar el tráfico en la red.

## Agregar controladores para el Entorno de preinstalación de Windows (WinPE)

*Para agregar controladores para el Entorno de preinstalación de Windows (WinPE):*

1. En la carpeta **Instalación remota** del árbol de la consola, seleccione la subcarpeta **Desplegar imágenes de dispositivo**.

2. En el espacio de trabajo de la carpeta **Desplegar imágenes de dispositivo**, haga clic en el botón **Acciones adicionales** y seleccione **Configurar conjunto de controladores para el Entorno de preinstalación de Windows (WinPE)** en la lista desplegable.

   Se abrirá la ventana **Controladores del Entorno de preinstalación de Windows**.

3. En el botón **Controladores del Entorno de preinstalación de Windows** haga clic en la ventana **Agregar**.

   Se abre la ventana **Seleccionar controlador**.

4. En la ventana **Seleccionar controlador**, seleccione un controlador de la lista.

   Si el controlador necesario no figura en la lista, haga clic en el botón **Agregar** y especifique el nombre del controlador y la carpeta del paquete de distribución de controladores en la ventana **Agregar controlador** que se abra.

   Para seleccionar una carpeta, haga clic en el botón **Examinar**.

   En la ventana **Agregar controlador**, haga clic en **Aceptar**.

5. En la ventana **Seleccionar controlador**, haga clic en **Aceptar**.

   El controlador se agregará al repositorio del Servidor de administración. Cuando se agrega al repositorio, el controlador se muestra en la ventana **Seleccionar controlador**.

6. En la ventanade **Controladores del Entorno de preinstalación de Windows**, haga clic en **Aceptar**.

El controlador se agregará al Entorno de preinstalación de Windows (WinPE).

## Agregar controladores a un paquete de instalación con una imagen del sistema operativo

*Para agregar controladores a un paquete de instalación con una imagen del sistema operativo, realice lo siguiente:*

1. En la carpeta **Instalación remota** del árbol de la consola, seleccione la subcarpeta **Paquetes de instalación**.

2. Desde el menú contextual de un paquete de instalación con una imagen del sistema operativo, seleccione **Propiedades**.

   Se abre la ventana de propiedades del paquete de instalación.

3. En la ventana de propiedades del paquete de instalación, seleccione la sección **Controladores adicionales**.

4. Haga clic en el botón **Agregar** en la sección **Controladores adicionales**.

   Se abre la ventana **Seleccionar controlador**.

5. En la ventana **Seleccionar controlador**, seleccione los controladores que desea agregar al paquete de instalación con la imagen de sistema operativo.

   Puede agregar los nuevos controladores al repositorio del Servidor de administración haciendo clic en el botón **Agregar** en la ventana **Seleccionar controlador**.

6. Haga clic en **Aceptar**.

Los controladores agregados se muestran en la sección **Controladores adicionales** de la ventana de propiedades del paquete de instalación con la imagen del sistema operativo.

## Configurar la utilidad sysprep.exe

La utilidad sysprep.exe está destinada a preparar al dispositivo para la creación de una imagen del sistema operativo.

*Para configurar la utilidad sysprep.exe, realice lo siguiente:*

1. En la carpeta **Instalación remota** del árbol de la consola, seleccione la subcarpeta **Paquetes de instalación**.

2. Desde el menú contextual de un paquete de instalación con una imagen del sistema operativo, seleccione **Propiedades**.

   Se abre la ventana de propiedades del paquete de instalación.

3. En la ventana de propiedades del paquete de instalación, seleccione la sección **Configuración de sysprep.exe**.

4. En la sección **Configuración de sysprep.exe**, indique qué archivo de configuración se usará al desplegar el sistema operativo en el dispositivo cliente:

   - **Usar archivo de configuración predeterminado**. Seleccione esta opción para usar el archivo de respuesta generado de forma predeterminada durante la captura de la imagen del sistema operativo.

   - **Personalizar valores de configuración principales**. Seleccione esta opción para especificar valores para la configuración a través de la interfaz del usuario.

   - **Especificar el archivo de configuración**. Seleccione esta opción para usar un archivo de respuesta personalizado.

5. Para aplicar los cambios realizados, haga clic en el botón **Aplicar**.

# Instalar sistemas operativos en dispositivos nuevos de la red

*Para instalar de forma remota un sistema operativo en dispositivos nuevos que aún no tengan ningún sistema operativo instalado:*

1. En la carpeta **Instalación remota** del árbol de la consola, seleccione la subcarpeta **Desplegar imágenes de dispositivo**.

   Cerciórese de que la opción **Mostrar Administración de vulnerabilidades y parches** esté activada en la ventana **Configuración de interfaz**. De lo contrario, la carpeta **Instalación remota** no se muestra.

2. Haga clic en el botón **Acciones adicionales** y seleccione **Administrar la lista de servidores PXE en la red** en la lista desplegable.

   La ventana **Propiedades**: **Desplegar imágenes de dispositivos** se abre, en la que se muestra la sección **Servidores PXE**.

3. En la sección **Servidores PXE**, haga clic en el botón **Agregar** y, en la ventana **Servidores PXE** que se abre, seleccione el dispositivo que se utilizará como el servidor PXE.

   El dispositivo que agregó se muestra en la sección de servidores PXE. Los archivos WinPE creados se transfieren al dispositivo desde el Servidor de administración. El proceso de transferencia de archivos suele tomar 10 minutos. Una vez que se completa la transferencia, el valor que se muestra en **Estado** cambia de **Guía de inicio rápido** a **Listo**.

4. En la sección **Servidores PXE**, seleccione un servidor PXE y haga clic en el botón **Propiedades**.

5. En la ventana Propiedades del servidor PXE seleccionado, en la pestaña **Configuración de conexión del servidor PXE** configure la conexión entre el Servidor de administración y el servidor PXE.

6. Inicie el dispositivo cliente en el que desee instalar el sistema operativo.

7. En BIOS del dispositivo cliente, seleccione la opción de instalación de inicio de la Red.

   El dispositivo cliente se conecta al servidor PXE y se muestra luego en el espacio de trabajo de la carpeta **Desplegar imágenes de dispositivo**.

8. En la sección **Acciones**, haga clic en el enlace **Asignar paquete de instalación** para seleccionar el paquete de instalación que se utilizará para instalar el sistema operativo en el dispositivo seleccionado.

   Utilice la herramienta DiskPart en el dispositivo seleccionado para comprobar los discos disponibles. En el símbolo del sistema de Windows PE, escriba `diskpart` para abrir la herramienta DiskPart. Tipo `list disk` para listar los discos.

   Después de agregar el dispositivo y asignarle el paquete de instalación, la instalación del sistema operativo comienza automáticamente en el dispositivo.

9. Para cancelar la instalación del sistema operativo en el dispositivo cliente, haga clic en el enlace **Cancelar instalación de imagen de SO** en la sección **Acciones**.

*Para agregar dispositivos por dirección MAC:*

- En la carpeta **Desplegar imágenes de dispositivo**, haga clic en **Agregar la dirección MAC de un dispositivo** para abrir la ventana **Nuevo dispositivo** y especificar la dirección MAC del dispositivo que desea agregar.

- En la carpeta **Desplegar imágenes de dispositivo**, haga clic en **Importar direcciones MAC de dispositivos desde un archivo** para seleccionar el archivo que contiene una lista de direcciones MAC de todos los dispositivos en los cuales desee instalar un sistema operativo.

## Instalar sistemas operativos en dispositivos cliente

*Para instalar un sistema operativo de manera remota en dispositivos cliente que ya tengan otro sistema operativo instalado:*

1. En el árbol de la consola, abra la carpeta **Instalación remota** y haga clic en el vínculo **Desplegar paquete de instalación a los dispositivos administrados (estaciones de trabajo)** para ejecutar el Asistente de despliegue de la protección.

2. En la ventana **Seleccionar paquete de instalación** del Asistente, especifique paquete de instalación con una imagen del sistema operativo.

3. Siga las instrucciones del asistente.

Cuando el Asistente completa su operación, una tarea de instalación remota se crea para la instalación del sistema operativo en dispositivos cliente. Puede iniciar o detener la tarea en la carpeta **Tareas**.

## Crear paquetes de instalación de aplicaciones

*Para crear un paquete de instalación de la aplicación:*

1. En la carpeta **Instalación remota** del árbol de la consola, seleccione la subcarpeta **Paquetes de instalación**.

2. Haga clic en el botón **Crear paquete de instalación** para ejecutar el Asistente de nuevo paquete.

3. En la ventana **Seleccione un tipo de paquete de instalación** del asistente, haga clic en uno de los siguientes botones:

- **Crear un paquete de instalación para una aplicación de Kaspersky**. Seleccione esta opción si desea crear un paquete de instalación para una aplicación de Kaspersky.

- **Crear un paquete de instalación para el archivo ejecutable especificado**. Seleccione esta opción si desea crear un paquete de instalación para una aplicación desarrollada por un tercero a partir de un archivo ejecutable. Por lo general, el archivo ejecutable que se utiliza en estos casos es el de instalación del programa.

  - Copiar toda la carpeta al paquete de instalación

    Seleccione esta opción si el archivo ejecutable está acompañado de otros que también se requieren para instalar la aplicación. Antes de habilitar esta opción, asegúrese de que todos los archivos pertinentes estén almacenados en la misma carpeta. Si habilita esta opción, la aplicación agregará todo el contenido de la carpeta, incluido el archivo ejecutable especificado, al paquete de instalación.

  - Especificar parámetros de instalación

    En la mayoría de los casos, para que una aplicación se instale en forma remota correctamente, la instalación se debe realizar en modo silencioso. Para instalar una aplicación en modo silencioso, es necesario especificar el parámetro pertinente.

    Configure los parámetros de instalación:

    - **Línea de comandos para el archivo ejecutable**

      Si la aplicación requiere un parámetro adicional para instalarse en modo silencioso, especifíquelo en este campo. Para más detalles, consulte la documentación del proveedor.

      También puede introducir otros parámetros.

    - **Convertir valores de configuración a los recomendados para las aplicaciones que Kaspersky Security Center reconoce**

      Si la base de datos de Kaspersky contiene la información pertinente, la aplicación se instalará con los parámetros recomendados.

      Dichos parámetros reemplazarán a los que pueda haber indicado en el campo **Línea de comandos para el archivo ejecutable**.

      Esta opción está activada de forma predeterminada.

      La creación y el mantenimiento de la base de datos de Kaspersky está a cargo de nuestros analistas. Cada vez que agregan una aplicación a la base de datos, los analistas de Kaspersky determinan cuáles son sus parámetros de instalación óptimos. Los parámetros se eligen para garantizar que la aplicación pueda instalarse sin problemas en un dispositivo cliente remoto. La base de datos se actualiza automáticamente en el Servidor de administración cuando se ejecuta la tarea del Servidor de administración Descargar actualizaciones en el repositorio.

- **Seleccionar una aplicación de la base de datos de Kaspersky para crear un paquete de instalación**. Seleccione esta opción si, para crear el paquete de instalación, desea seleccionar una aplicación desarrollada por un tercero en la base de datos de Kaspersky. La base de datos se crea automáticamente cuando se ejecuta la tarea del Servidor de administración Descargar actualizaciones en el repositorio. Las aplicaciones se muestran en la lista.

- **Cree un paquete de instalación con la imagen del sistema operativo**. Seleccione esta opción si necesita crear un paquete de instalación con una imagen del sistema operativo de un dispositivo de referencia.

  Cuando el Asistente finaliza, se crea una tarea del Servidor de administración con el nombre **Crear un paquete de instalación basado en la imagen del SO de un dispositivo de referencia**. Cuando se completa esta tarea, se crea un paquete de instalación que puede usar para instalar la imagen del sistema operativo a través de un servidor PXE o con la tarea de instalación remota.

4. Siga las instrucciones del asistente.

Cuando el Asistente finaliza, se crea un paquete de instalación que puede usar para instalar la aplicación en dispositivos cliente. Para ver el paquete de instalación, seleccione **Paquetes de instalación** en el árbol de la consola.

## Emitir un certificado para paquetes de instalación de aplicaciones

*Para emitir un certificado para el paquete de instalación de una aplicación:*

1. En la carpeta **Instalación remota** del árbol de la consola, seleccione la subcarpeta **Paquetes de instalación**.

   De manera predeterminada, la carpeta **Instalación remota** es una subcarpeta de la carpeta **Avanzado**.

2. En el menú contextual de la carpeta **Paquetes de instalación** seleccione **Avanzado**.

   Esto abre la ventana de propiedades de la carpeta **Paquetes de instalación**.

3. En la ventana de propiedades de la carpeta **Paquetes de instalación**, seleccione la sección **Firmar paquetes independientes**.

4. En la sección **Firmar paquetes independientes**, haga clic en el botón **Especificar**.

   La ventana **Certificado**.

5. En el campo **Tipo de certificado**, especifique el tipo de certificado público o privado:

   - Si está seleccionado el valor **Contenedor PKCS #12**, especifique el archivo de certificado y la contraseña.
   - Si está seleccionado el valor **Certificado X.509**:

     a. Especifique el archivo de clave privada (con las extensiones *.prk o *.pem).

     b. Especifique la contraseña de la clave privada.

     c. Especifique el archivo de clave pública (con la extensión *.cer).

6. Haga clic en **Aceptar**.

Se emite un certificado para el paquete de instalación de la aplicación.

## Instalar aplicaciones en dispositivos cliente

*Para instalar una aplicación en dispositivos cliente:*

1. En el árbol de la consola, abra la carpeta **Instalación remota** y haga clic en **Desplegar paquete de instalación a los dispositivos administrados (estaciones de trabajo)** para ejecutar el Asistente de despliegue de la protección.

2. En la ventana **Seleccionar paquete de instalación** del Asistente, especifique el paquete de instalación de una aplicación que desee instalar.

3. Siga las instrucciones del asistente.

Cuando el Asistente finaliza, una tarea de instalación remota se crea para la instalación de la aplicación en los dispositivos cliente. Puede iniciar o detener la tarea en la carpeta **Tareas**.

Usando el Asistente de despliegue de la protección, puede instalar el Agente de red en dispositivos cliente que ejecuten Windows, Linux y macOS.

Para administrar aplicaciones de seguridad de 64 bits usando Kaspersky Security Center en dispositivos que ejecuten sistemas operativos de Linux, debe usar Agente de red de 64 bits para Linux. Puede descargar la versión necesaria del Agente de red desde el Sitio web del Servicio de soporte técnico.

Antes de la instalación remota del Agente de red en un dispositivo que ejecuta Linux, debe preparar el dispositivo.

# Administración de revisiones de objetos

En esta sección encontrará información sobre la administración de revisiones de objetos. Kaspersky Security Center permite que usted siga la modificación de objeto. Cuando un objeto se modifica de algún modo, se crea una *revisión*. Cada revisión lleva un número que la identifica.

Los objetos de aplicación que admiten la administración de la revisión incluyen:

- Propiedades del Servidor de administración
- Directivas
- Tareas
- Grupos de administración
- Cuentas de usuario
- Paquetes de instalación

Puede realizar las siguientes acciones con las revisiones de los objetos:

- Comparar una revisión seleccionada con la actual
- Comparar revisiones seleccionadas
- Comparar un objeto con una revisión seleccionada de otro objeto del mismo tipo
- Ver una revisión específica
- Deshacer los cambios realizados en un objeto y hacer que este revierta su estado al de una revisión específica
- Guardar revisiones como archivo .txt

Todo objeto compatible con la administración de revisiones tiene una sección llamada **Historial de revisiones** en su ventana de propiedades. La sección contiene una lista de revisiones asociadas al objeto y los siguientes datos:

- Número de revisión del objeto
- Fecha y hora de modificación del objeto
- Nombre del usuario que modificó el objeto
- Acción realizada en el objeto
- Descripción de la revisión vinculada al cambio en la configuración del objeto

## Acerca de las revisiones de objetos

Puede realizar las siguientes acciones con las revisiones de los objetos:

- Comparar una revisión seleccionada con la actual
- Comparar revisiones seleccionadas
- Comparar un objeto con una revisión seleccionada de otro objeto del mismo tipo
- Ver una revisión específica
- Deshacer los cambios realizados en un objeto y hacer que este revierta su estado al de una revisión específica
- Guardar revisiones como archivo .txt

Todo objeto compatible con la administración de revisiones tiene una sección llamada **Historial de revisiones** en su ventana de propiedades. La sección contiene una lista de revisiones asociadas al objeto y los siguientes datos:

- Número de revisión del objeto
- Fecha y hora de modificación del objeto
- Nombre del usuario que modificó el objeto

- Acción realizada en el objeto
- Descripción de la revisión vinculada al cambio en la configuración del objeto

## Visualización de la sección Historial de revisión

Puede comparar revisiones de un objeto a la revisión actual, comparar revisiones diferentes seleccionadas en la lista o comparar una revisión de un objeto a una revisión de otro objeto del mismo tipo.

*Para ver la sección **Historial de revisiones** de un objeto:*

1. En el árbol de consola, seleccione uno de los siguientes objetos:
   - Nodo **Servidor de administración**
   - Carpeta **Directivas**
   - Carpeta **Tareas**
   - Carpeta de un grupo de administración
   - Carpeta **Cuentas de usuario**
   - Carpeta **Objetos eliminados**
   - Subcarpeta **Paquetes de instalación**, que se anida en la carpeta **Instalación remota**
2. Según la ubicación del objeto relevante, realice una de las siguientes acciones:
   - Si el objeto está en el nodo del **Servidor de administración** o en un nodo del grupo de administración, haga clic con el botón derecho en el nodo y, en el menú contextual, seleccione **Propiedades**.
   - Si el objeto está en la carpeta **Directivas**, **Tareas**, **Cuentas de usuario**, **Objetos eliminados** o **Paquetes de instalación**, seleccione la carpeta y en el espacio de trabajo correspondiente seleccione el objeto.

   Se abre la ventana de propiedades de objeto.
3. En el panel **Secciones** de la izquierda, seleccione **Historial de revisiones**.

   El historial de revisiones se muestra en el espacio de trabajo.

## Comparación de revisiones de objetos

Puede comparar revisiones anteriores de un objeto con la revisión actual, comparar revisiones diferentes seleccionadas en la lista o comparar una revisión de un objeto con una revisión de otro objeto del mismo tipo.

*Para comparar las revisiones de un objeto:*

1. Seleccione un objeto y vaya a la ventana de propiedades del objeto.
2. En la ventana de propiedades, vaya a la sección **Historial de revisiones**.

3. En el espacio de trabajo, en la lista de revisiones de objeto, seleccione la revisión para la comparación.

   Para seleccionar más de una revisión del objeto, use las teclas **Mayús** y **Ctrl**.

4. Realice una de las siguientes acciones:

   - Haga clic en el botón **Comparar** y seleccione uno de los valores en la lista desplegable.

     - Comparar a revisión actual

       Seleccione esta opción para comparar la revisión seleccionada con la actual.

     - Comparar revisiones seleccionadas

       Seleccione esta opción de comparar dos revisiones seleccionadas.

     - Comparar con otra tarea

       Si trabaja con revisiones de tarea, seleccione **Comparar con otra tarea** para comparar la revisión seleccionada de una revisión de otra tarea.

       Si trabaja con revisiones de directivas, seleccione **Comparar con otra directiva** para comparar la revisión seleccionada con una revisión de otra directiva.

   - Haga doble clic en el nombre de una revisión y, en la ventana de propiedades de la revisión que se abre, haga clic en uno de los siguientes botones:

     - Comparar con actual

       Haga clic en este botón para comparar la revisión seleccionada con la actual.

     - Comparar con anterior

       Haga clic en este botón para comparar la revisión seleccionada con una anterior.

   Se muestra un informe en formato HTML sobre la comparación de las revisiones en su navegador predeterminado.

   En este informe, puede minimizar algunas secciones que contengan la configuración de revisiones. Para minimizar una sección con la configuración de la revisión de objeto, haga clic en el icono( ) al lado del nombre de la sección.

Las revisiones del Servidor de administración incluyen todos los detalles de cambios realizados, excepto la información de las siguientes áreas:

- Sección **Tráfico**
- Sección **Reglas de etiquetado**
- Sección **Notificación**

- Sección **Puntos de distribución**
- Sección **Brote de virus**

  No hay información registrada de la sección **Brote de virus** sobre la configuración de la activación de la directiva que se produce cuando se activa un evento de foco de virus.

Puede comparar las revisiones de un objeto eliminado con una revisión de un objeto existente, pero no a la inversa: no puede comparar las revisiones de un objeto existente con una revisión de un objeto eliminado.

## Configuración del plazo de almacenamiento de revisiones de objetos y de información de objetos eliminados

El plazo de almacenamiento para revisiones de objeto y para información sobre objetos eliminados es lo mismo. El plazo de almacenamiento predeterminado es de 90 días. Esto es suficiente tiempo para la auditoría habitual del programa.

Solo los usuarios con el permiso **Modificar** en el área de **Objetos eliminados** puede cambiar el periodo de almacenamiento.

*Para cambiar el plazo de almacenamiento para las revisiones de objetos y para obtener información sobre los objetos eliminados:*

1. En el árbol de la consola, seleccione el Servidor de administración para el que desea cambiar el periodo de almacenamiento.
2. Haga clic derecho y en el menú contextual seleccione **Propiedades**.
3. En la ventana de propiedades del Servidor de administración que se abre, en la sección **Repositorio del historial de revisiones**, introduzca el periodo de almacenamiento deseado (el número de días).
4. Haga clic en **Aceptar**.

Las revisiones de objetos y la información sobre los objetos eliminados se almacenarán durante el número de días que introdujo.

## Visualización de una revisión de objetos

Si tiene que saber qué modificaciones se hicieron a un objeto durante cierto período de tiempo, puede ver las revisiones de este objeto.

*Para ver las revisiones de un objeto:*

1. Vaya a la sección **Historial de revisiones** del objeto.
2. En la lista de revisiones del objeto, seleccione la revisión cuya configuración desea ver.
3. Realice una de las siguientes acciones:
   - Haga clic en el botón **Ver revisión**.
   - Abra la ventana de propiedades de la revisión haciendo doble clic sobre el nombre de la revisión y, luego, haciendo clic en el botón **Ver revisión**.

Un informe en el formato de HTML con la configuración de la revisión de objeto seleccionada se muestra. En este informe, puede minimizar algunas secciones con la configuración de la revisión de objeto. Para minimizar una sección con la configuración de la revisión de objeto, haga clic en el icono( ) al lado del nombre de la sección.

## Almacenamiento de una revisión de objetos en un archivo

Puede guardar una revisión de objeto como un archivo de texto, por ejemplo, a fin de enviarlo por correo electrónico.

*Para guardar una revisión de objeto en un archivo:*

1. Vaya a la sección **Historial de revisiones** del objeto.
2. En la lista de revisiones de un objeto, seleccione el objeto cuya configuración desea guardar.
3. Haga clic en el botón **Avanzado** y seleccione el valor **Guardar en archivo** en la lista desplegable.

La revisión se guarda como ahora un archivo .txt.

## Reversión de cambios

Los cambios realizados en un objeto pueden revertirse. Por ejemplo, puede volver a dejar la configuración de una directiva tal como estaba en una fecha puntual.

*Para revertir los cambios realizados en un objeto:*

1. Vaya a la sección **Historial de revisiones** del objeto.
2. En la lista de revisiones del objeto, seleccione el número de revisión a la que desee regresar.
3. Haga clic en el botón **Avanzado** y seleccione el valor **Revertir** en la lista desplegable.

El objeto volverá a la revisión seleccionada. La lista de revisiones del objeto mostrará un registro de la acción que se tomó. En la descripción de la revisión, verá especificado el número de revisión a la que haya regresado el objeto.

## Agregar una descripción a una revisión

Para ayudarse a encontrar una revisión específica en la lista, puede agregarle una descripción.

*Para agregar una descripción a una revisión:*

1. Vaya a la sección **Historial de revisiones** del objeto.
2. En la lista de revisiones del objeto, seleccione la revisión a la que desea agregar la descripción.
3. Haga clic en el botón **Descripción**.

4. En la ventana **Descripción de la revisión de objetos**, puede agregar una descripción de revisión.

   De forma predeterminada, la descripción de las revisiones está en blanco.

5. Haga clic en **Aceptar**.

# Eliminación de objetos

Esta sección proporciona información sobre cómo eliminar objetos.

Puede eliminar objetos como los siguientes:

- Directivas
- Tareas
- Paquetes de instalación
- Servidores de administración virtuales
- Usuarios
- Grupos de seguridad
- Grupos de administración

*Para eliminar un objeto:*

1. Abra la sección correspondiente de Kaspersky Security Center Web Console y luego seleccione el objeto.
2. En la barra de herramientas, haga clic en el botón **Eliminar**.
3. En la ventana que se abre, haga clic en **Aceptar** para confirmar su selección.

   Se elimina el objeto seleccionado.

Cuando se elimina un objeto, se conserva información sobre el mismo en la base de datos. El plazo de almacenamiento para la información sobre los objetos eliminados es el mismo que el plazo de almacenamiento para las revisiones de objetos (el plazo recomendado es de 90 días). Puede cambiar el plazo de almacenamiento solo si tiene el permiso **Modificar** en el área de derechos **Objetos eliminados**.

## Acercad de la eliminación de dispositivos cliente

Cuando elimina un dispositivo administrado de un grupo de administración, la aplicación mueve el dispositivo al grupo de Dispositivos no asignados. Después de eliminar el dispositivo, las aplicaciones de Kaspersky instaladas (Agente de red y cualquier aplicación de seguridad, por ejemplo, Kaspersky Endpoint Security) permanecen en el dispositivo.

Kaspersky Security Center maneja los dispositivos del grupo Dispositivos no asignados según las siguientes reglas:

- Si configuró reglas de movimiento de dispositivos y un dispositivo cumple con los criterios de una regla de movimiento, el dispositivo se mueve automáticamente a un grupo de administración de acuerdo con la regla.

- El dispositivo se almacena en el grupo de Dispositivos no asignados y se elimina automáticamente del grupo de acuerdo con las reglas de retención de dispositivos.

  Las reglas de retención de dispositivos no afectan a los dispositivos que tienen una o más unidades cifradas con cifrado de disco completo. Dichos dispositivos no se eliminan automáticamente, solo puede hacerlo de forma manual. Si necesita eliminar un dispositivo con una unidad cifrada, primero descifre la unidad y, luego, elimine el dispositivo.

  > Cuando elimina un dispositivo que tiene una unidad cifrada, también se eliminan los datos necesarios para descifrar la unidad. Si selecciona la casilla **Comprendo el riesgo y deseo eliminar los dispositivos seleccionados** en la ventana de confirmación que se abre cuando elimina dichos dispositivos (ya sea del grupo **Dispositivos no asignados** o **Dispositivos administrados**), significa que está al tanto de la subsecuente eliminación de datos.

  Para descifrar la unidad, se deben cumplir las siguientes condiciones:

  - El dispositivo se vuelve a conectar al Servidor de administración para restaurar los datos necesarios para descifrar la unidad.

  - El usuario del dispositivo recuerda la contraseña de descifrado.

  - La aplicación de seguridad que se usó para cifrar la unidad, por ejemplo, Kaspersky Endpoint Security para Windows, todavía está instalada en el dispositivo.

  Si la tecnología Kaspersky Disk Encryption descifró la unidad, también puede intentar recuperar los datos con la utilidad de restauración FDERT.

> En VDI, si tiene un dispositivo con unidades cifradas, la información de la unidad cifrada se elimina después de eliminar el dispositivo.

Cuando elimina manualmente un dispositivo del grupo de Dispositivos no asignados, la aplicación elimina el dispositivo de la lista. Después de eliminar el dispositivo, las aplicaciones de Kaspersky instaladas (si las hay) permanecen en el dispositivo. Después, si el dispositivo sigue estando visible para el Servidor de administración y ha configurado un sondeo de red regular, Kaspersky Security Center detecta el dispositivo durante el sondeo de red y lo agrega nuevamente al grupo Dispositivos no asignados. Por lo tanto, es razonable eliminar un dispositivo manualmente solo si el servidor de administración no puede ver el dispositivo.

## Eliminar objeto

Puede eliminar objetos como directivas, tareas, paquetes de instalación, usuarios internos y grupos de seguridad internos si tiene permiso de Modificar, que se encuentra en la categoría de derechos de Funcionalidad básica (consulte el artículo Asignar permisos a usuarios y grupos para obtener más información).

No puede eliminar los paquetes de instalación que se utilizan en las tareas de instalación remota. Primero debe detener las tareas correspondientes. Para obtener más información sobre las tareas de instalación automática en un grupo de administración, consulte el artículo Instalación automática de aplicaciones en dispositivos de un grupo de administración.

*Para eliminar un objeto:*

1. En el árbol de la consola, en el espacio de trabajo de la carpeta requerida, seleccione un objeto.
2. Realice una de las siguientes acciones:
   - Haga clic con el botón derecho del ratón en el objeto y seleccione **Eliminar**.
   - Pulse la tecla **SUPRIMIR**.

El objeto se eliminará y la información sobre él se guardará en la base de datos.

## Visualización de información sobre los objetos eliminados

La información sobre los objetos eliminados se almacena en la carpeta Objetos eliminados durante la misma cantidad de tiempo que las revisiones de objetos (el periodo recomendado es de 90 días).

Solo los usuarios con permiso de **Lectura** en el área de derechos **Objetos eliminados** pueden ver la lista de objetos eliminados (consulte Asignación de permisos a usuarios y grupos para obtener más información).

*Para ver la lista de objetos eliminados,*

En el árbol de la consola, seleccione **Objetos eliminados** (de forma predeterminada, **Objetos eliminados** es una subcarpeta de la carpeta **Avanzado**).

Si no tiene permiso de lectura en el área de derechos **Objetos eliminados**, se mostrará una lista vacía en la carpeta **Objetos eliminados**.

El espacio de trabajo de la carpeta **Objetos eliminados** contiene la siguiente información sobre los objetos eliminados:

- **Nombre**. Nombre del objeto.
- **Tipo**. Tipo de objeto, como directiva, tarea o paquete de instalación.
- **Hora**. Hora a la que se eliminó el objeto.
- **Usuario**. Nombre de cuenta del usuario que eliminó el objeto.

*Para ver más información sobre un objeto:*

1. En el árbol de la consola, seleccione **Objetos eliminados** (de forma predeterminada, **Objetos eliminados** es una subcarpeta de la carpeta **Avanzado**).

2. En el espacio de trabajo **Objetos eliminados**, seleccione el objeto que desee.

   El cuadro para trabajar con el objeto seleccionado aparece en el lado derecho del espacio de trabajo.

3. Realice una de las siguientes acciones:

   - Haga clic en el enlace **Propiedades** en el cuadro.
   - Haga clic con el botón derecho en el objeto que seleccionó en el espacio de trabajo y, en el menú contextual, seleccione **Propiedades**.

   Se abre la ventana de propiedades del objeto, que muestra las siguientes pestañas:

   - **General**
   - **Historial de revisiones**

## Eliminar objetos permanentemente de la lista de objetos eliminados

Solo los usuarios con permiso **Modificar** en el área de derechos **Objetos eliminados** pueden eliminar objetos permanentemente de la lista de objetos eliminados (consulte Asignación de permisos a usuarios y grupos para obtener más información).

*Para eliminar objetos de la lista de objetos eliminados:*

1. En el árbol de la consola, seleccione el nodo del Servidor de administración necesario y después seleccione la carpeta **Objetos eliminados**.

2. En el espacio de trabajo, seleccione los objetos que desea eliminar.

3. Realice una de las siguientes acciones:

   - Pulse la tecla **SUPRIMIR**.
   - En el menú contextual de los objetos que seleccionó, seleccione **Eliminar**.

4. En la ventana de diálogo de confirmación, haga clic en **Sí**.

   El objeto se elimina permanentemente de la lista de objetos eliminados. Toda la información sobre este objeto (incluidas todas sus revisiones) se elimina permanentemente de la base de datos. No se puede restaurar esta información.

# Administración de dispositivos móviles

La administración de protección del dispositivo móvil a través de Kaspersky Security Center se realiza usando la función Administración de dispositivos móviles, que exige una licencia especializada. Si tiene la intención de administrar dispositivos móviles que son propiedad de los empleados de su organización, debe habilitar la Administración de dispositivos móviles.

Esta sección proporciona instrucciones para habilitar, configurar y deshabilitar la administración de dispositivos móviles. Esta sección también describe cómo administrar los dispositivos móviles conectados al Servidor de administración.

Para obtener detalles sobre Kaspersky Security for Mobile, consulte la *Ayuda de Kaspersky Security for Mobile*.

# Escenario: Despliegue de la característica Administración de dispositivos móviles

En esta sección se presenta un escenario para configurar la función Administración de dispositivos móviles en Kaspersky Security Center.

## Requisitos previos

Asegúrese de tener una licencia que le dé acceso a la función Administración de dispositivos móviles.

## Etapas

El proceso para poner en funcionamiento la característica Administración de dispositivos móviles se divide en etapas:

1. **Preparación de los puertos**

   Asegúrese de que el puerto 13292 esté disponible en el Servidor de administración. Dicho puerto se necesita para conectar los dispositivos móviles. También puede necesitarse el puerto 17100. Este puerto se requiere únicamente para el servidor proxy de activación de los dispositivos móviles administrados; si dichos dispositivos no tienen acceso a Internet, no es necesario que el puerto esté disponible.

2. **Habilitar Administración de dispositivos móviles**

   Puede activar la Administración de dispositivos móviles cuando ejecute el Asistente de inicio rápido del Servidor de administración o después.

3. **Especificación de la dirección externa del Servidor de administración**

   Puede especificar la dirección externa cuando ejecute el Asistente de inicio rápido del Servidor de administración o en otro momento. Si no seleccionó Administración de dispositivos móviles para la instalación y no especificó la dirección en el Asistente de instalación, especifique la dirección externa en las propiedades del paquete de instalación.

4. **Asignar los dispositivos móviles al grupo de dispositivos administrados**

   Añada los dispositivos móviles al grupo de dispositivos administrados para poder administrar estos dispositivos mediante directivas. Puede crear una regla de movimiento en uno de los pasos del Asistente de inicio rápido del Servidor de administración. También puede crear la regla de movimiento más tarde. Si no crea una regla de este tipo, puede agregar dispositivos móviles al grupo de dispositivos administrados manualmente.

   Puede agregar dispositivos móviles al grupo de dispositivos administrados directamente o puede crear un subgrupo (o varios subgrupos) para ellos.

   En cualquier momento posterior, puede conectar cualquier dispositivo móvil nuevo al Servidor de administración mediante el Asistente para conectar un nuevo dispositivo móvil.

5. **Crear una directiva para los dispositivos móviles**

Para administrar dispositivos móviles, cree una o varias directivas para ellos en los grupos a los que pertenecen. Puede cambiar la configuración de esta directiva en cualquier momento después.

### Resultados

Cuando haya completado las etapas de este escenario, estará en condiciones de administrar dispositivos Android y iOS a través de Kaspersky Security Center. Puede trabajar con certificados de dispositivos móviles y enviar comandos a dispositivos móviles.

## Acerca de la directiva de grupo para la administración de dispositivos MDM con iOS

Para administrar dispositivos MDM con iOS, puede utilizar el complemento de administración de Kaspersky Device Management para iOS, incluido en el kit de distribución de Kaspersky Security Center. Kaspersky Device Management para iOS le permite crear directivas de grupo para especificar los ajustes de configuración de los dispositivos MDM con iOS sin usar la Utilidad de configuración de iPhone®.

Una directiva de grupo para administrar dispositivos MDM con iOS le brinda al administrador las siguientes opciones:

- Configuración de la seguridad de la contraseña del dispositivo.
- Configuración de restricciones en el uso de características de hardware del dispositivo, sobre la instalación y eliminación de aplicaciones móviles.
- Configuración de las restricciones sobre el uso de aplicaciones móviles preinstaladas, tal como YouTube™, iTunes® Store o Safari.
- Configurar las restricciones de los contenidos multimedia que se ven (por ejemplo, películas y programas de TV) en función de la región en la que se encuentren los dispositivos.
- Configurar la conexión del dispositivo a Internet mediante servidores proxy (proxy HTTP global).
- Configurar las cuentas con las que los usuarios acceden a las aplicaciones y a los servicios corporativos (tecnología de inicio de sesión único (SSO)).
- Supervisión del uso de Internet (visitas a sitios web) en dispositivos móviles.
- Configurar redes inalámbricas (Wi-Fi), puntos de acceso (APN) y redes privadas virtuales (VPN) que utilizan distintos mecanismos de autenticación y protocolos de red.
- Configuración de la conexión a dispositivos AirPlay® para la transmisión de fotos, música y videos.
- Configuración de la conexión a impresoras AirPrint™ para la impresión inalámbrica de documentos desde el dispositivo.
- Configuración de la sincronización con el servidor Microsoft Exchange y cuentas de usuario para usar correo electrónico corporativo en los dispositivos.
- Configuración de credenciales de usuario para la sincronización con el servicio de directorio LDAP.
- Configurar las credenciales de usuario para que se conecten con los servicios de CalDAV y CardDAV que conceden a los usuarios acceso a los calendarios y a las listas de contactos corporativos.

- Ajustar configuración de la interfaz de iOS, como fuentes o iconos para sitios web favoritos, en el dispositivo del usuario.
- Adición de nuevos certificados de seguridad en dispositivos.
- Configuración del servidor del Protocolo simple de registro de certificados (SCEP) para la recuperación automática de los certificados por parte del dispositivo desde la autoridad de certificación.
- Adición de configuración personalizada para la operación de aplicaciones móviles.

Una directiva para administrar dispositivos MDM con iOS es especial, ya que se asigna a un grupo de administración que incluye el Servidor de MDM para iOS (llamado "Servidor de dispositivos móviles"). Todas las configuraciones especificadas en esta directiva se aplican en primer lugar a los servidores de dispositivos móviles y luego a los dispositivos móviles administrados por estos. En el caso de una estructura jerárquica de grupos de administración, los servidores de dispositivos móviles secundarios reciben la configuración de directivas de los servidores de dispositivos móviles principales y la distribuyen a los dispositivos móviles.

Para obtener más información sobre cómo usar la directiva de grupo a fin de administrar dispositivos MDM con iOS en la Consola de administración de Kaspersky Security Center, consulte la documentación de *Kaspersky Security para dispositivos móviles*.

## Habilitar Administración de dispositivos móviles

Para administrar dispositivos móviles, debe habilitar Administración de dispositivos móviles. Si no activó esta función en el Asistente de inicio rápido, puede activarla más adelante. Administración de dispositivos móviles requiere licencia.

> La activación de la Administración de dispositivos móviles solo está disponible en el Servidor de administración principal.

*Para habilitar la Administración de dispositivos móviles:*

1. En el árbol de la consola, seleccione la carpeta **Administración de dispositivos móviles**.
2. En el espacio de trabajo de la carpeta, haga clic en el botón **Habilitar Administración de dispositivos móviles**. Este botón solo está disponible si no ha activado antes la **Administración de dispositivos móviles**.

   Se muestra la página **Componentes adicionales** del Asistente de inicio rápido del Servidor de administración.
3. Seleccione **Habilitar Administración de dispositivos móviles** para poder administrar dispositivos móviles.
4. En la página **Seleccione un método para activar la aplicación**, active la aplicación usando un archivo de clave o un código de activación.

   La administración de dispositivos móviles no será posible a menos que active la función Administración de dispositivos móviles.
5. En la página **Configuración del servidor proxy para obtener acceso a Internet**, seleccione la casilla de verificación **Usar servidor proxy** si desea usar un servidor proxy al conectarse a Internet. Cuando esta casilla de verificación está seleccionada, los campos están disponibles para introducir la configuración. Especifique la configuración para la conexión del servidor proxy.

6. En la página **Búsqueda de actualizaciones para complementos y paquetes de instalación**, seleccione una de las siguientes opciones:

   - **Comprobar si los complementos y los paquetes de instalación están actualizados**

     Iniciando el chequeo de estado actualizado. Si el chequeo detecta versiones desactualizadas de algunos complementos o paquetes de instalación, el Asistente le solicita descargar versiones actualizadas para reemplazarlas.

   - **Omitir comprobación**

     Seguir trabajando sin verificar si los paquetes de instalación y componentes están actualizados. Puede seleccionar esta opción si, por ejemplo, no tiene Acceso a Internet o si desea realizar la versión anticuada de la aplicación por la razón que sea.

     Saltar el chequeo de actualizaciones para complementos puede causar el funcionamiento impropio de la aplicación.

7. En la página **Últimas versiones de complementos disponibles**, descargue e instale las últimas versiones de complementos en el idioma que su versión de la aplicación requiere. La actualización de los complementos no requiere una licencia.

   Después de que instala los complementos y paquetes, los chequeos de aplicación si todos los complementos requeridos para el correcto funcionamiento de dispositivos móviles se han instalado. Si se detectan versiones desactualizadas de algunos complementos, el Asistente le solicita descargar versiones actualizadas para reemplazarlas.

8. En la página **Parámetros para la conexión de dispositivos móviles**, configure los puertos del Servidor de administración.

Cuando el Asistente finalice, se realizarán los siguientes cambios:

- Se creará la directiva de Kaspersky Endpoint Security para Android.
- Se creará la directiva de Kaspersky Device Management for iOS.
- Los puertos se abrirán en el Servidor de administración para dispositivos móviles.

## Modificar la configuración de administración de dispositivos móviles

*Para habilitar la compatibilidad de dispositivos móviles:*

1. En el árbol de la consola, seleccione la carpeta **Administración de dispositivos móviles**.
2. En el espacio de trabajo de esta carpeta, haga clic en el enlace **Puertos de conexión para dispositivos móviles**.

   La sección **Puertos adicionales** de la ventana Propiedades del Servidor de administración se muestra.

3. En la sección **Puertos adicionales**, modifique la configuración correspondiente:

   - **Puerto SSL para el servidor proxy de activación**
   - **Abrir puerto para dispositivos móviles**

     Se abrirá un puerto para que los dispositivos móviles se conecten al Servidor de administración de licencias. Si desea definir el número de puerto y otros ajustes, podrá hacerlo en los campos de abajo.

     Esta opción está activada de forma predeterminada.

   - **Puerto para la sincronización del dispositivo móvil**

     Número del puerto que los dispositivos móviles usarán para establecer conexión e intercambiar datos con el Servidor de administración. El número de puerto predeterminado es 13292.

     Puede asignar un puerto diferente si utiliza el puerto 13292 para otros fines.

   - **Puerto para la activación de dispositivos móviles**

     Puerto que Kaspersky Endpoint Security para Android usará para conectarse con los servidores de activación de Kaspersky.

     El número de puerto predeterminado es 17100.

4. Haga clic en **Aceptar**.

## Deshabilitar la administración de dispositivos móviles

La desactivación de la Administración de dispositivos móviles solo está disponible en el Servidor de administración principal.

*Para deshabilitar la administración de dispositivos móviles*

1. En el árbol de la consola, seleccione la carpeta **Administración de dispositivos móviles**.
2. En el espacio de trabajo de esta carpeta, haga clic en el enlace **Configurar componentes adicionales**

   Se muestra la página **Componentes adicionales** del Asistente de inicio rápido del Servidor de administración.
3. Seleccione **No habilitar la administración de dispositivos móviles** si ya no desea administrar dispositivos móviles.
4. Haga clic en **Aceptar**.

Los dispositivos móviles conectados antes de esta acción no podrán conectarse al Servidor de administración. El puerto para la conexión del dispositivo móvil y el puerto para la activación de los dispositivos móviles se cerrarán automáticamente.

Las directivas que se hayan creado para Kaspersky Endpoint Security para Android y Kaspersky Device Management for iOS no se eliminarán. Las reglas de la emisión del certificado no se modificarán. Los complementos instalados no se eliminarán. La regla de movimiento de dispositivos móviles no se eliminará.

Después de que vuelve a activar la Administración de dispositivos móviles administrados, puede que deba volver a instalar aplicaciones móviles que se requieran para la administración de dispositivos móviles.

# Trabajar con comandos para dispositivos móviles

Esta sección contiene información sobre los comandos para la administración de dispositivos móviles admitidos por Kaspersky Security Center. La sección proporciona instrucciones sobre cómo enviar comandos a dispositivos móviles, además de cómo ver los estados de ejecución de los comandos en el registro de comandos.

## Comandos para la administración de dispositivos móviles

Kaspersky Security Center admite comandos para la administración de dispositivos móviles.

Estos comandos se utilizan para la administración remota de dispositivos móviles. En caso de perderse un dispositivo móvil, por ejemplo, se puede utilizar un comando para eliminar todos los datos corporativos del dispositivo.

Puede usar comandos para los siguientes tipos de dispositivos móviles administrados:

- Dispositivos MDM con iOS
- Dispositivos con Kaspersky Endpoint Security (KES)

Cada tipo de dispositivo es compatible con un conjunto de comandos específico.

## Consideraciones especiales para ciertos comandos

- Cuando el comando **Restablecer ajustes de fábrica** se ejecuta correctamente en un dispositivo de cualquier tipo, se eliminan todos los datos del dispositivo y se restaura la configuración de fábrica del dispositivo.
- Cuando el comando **Eliminar datos corporativos** se ejecuta correctamente en un dispositivo MDM con iOS, se eliminan del dispositivo los perfiles de configuración instalados, los perfiles de aprovisionamiento, el perfil de MDM para iOS y las aplicaciones para las que se ha activado la casilla **Eliminar junto con el perfil de MDM para iOS**.
- Cuando el comando **Eliminar datos corporativos** se ejecuta correctamente en un dispositivo KES, se eliminan del dispositivo todos los datos corporativos, las entradas de la lista de contactos, el historial de mensajes SMS, el registro de llamadas, el calendario, los ajustes de conexión a Internet y las cuentas de usuario (excepto la cuenta de Google™). En dispositivos KES, el comando también borra todos los datos de la tarjeta de memoria.
- Antes de enviar el comando **Localizar** a un dispositivo KES, tendrá que confirmar que el comando se usará para hacer una búsqueda autorizada de un dispositivo perdido perteneciente a la organización o a uno de sus empleados. Un dispositivo móvil que recibe el comando **Localizar** no está bloqueado.

# Lista de comandos para dispositivos móviles

## La siguiente tabla contiene los comandos disponibles para dispositivos MDM con iOS.

Comandos disponibles para la administración de dispositivos móviles: dispositivos MDM con iOS

| Comandos | Resultado de la ejecución del comando |
|---|---|
| Bloquear | El dispositivo móvil se bloquea. |
| Desbloquear | Se deshabilita el bloqueo del dispositivo móvil con código PIN. Se elimina el código PIN configurado. |
| Restablecer ajustes de fábrica | Se eliminan todos los datos del dispositivo móvil y se restaura la configuración de fábrica. |
| Eliminar datos corporativos | Se eliminan todos los perfiles de configuración instalados, los perfiles de aprovisionamiento, el perfil de MDM para iOS y las aplicaciones para las que se ha activado la casilla **Eliminar junto con el perfil de MDM para iOS**. |
| Sincronizar dispositivo | Los datos del dispositivo móvil se sincronizan con el Servidor de administración. |
| Instalar perfil | El perfil de configuración se instala en el dispositivo móvil. |
| Eliminar perfil | El perfil de configuración se elimina del dispositivo móvil. |
| Instalar perfil de aprovisionamiento | El perfil de aprovisionamiento se instala en el dispositivo móvil. |
| Eliminar perfil de aprovisionamiento | El perfil de aprovisionamiento se elimina del dispositivo móvil. |
| Instalar app | La app se instala en el dispositivo móvil. |
| Eliminar app | La app se elimina del dispositivo móvil. |
| Ingresar código de canje | Se introduce un código de canje para una app paga. |
| Configurar roaming | Se habilita o deshabilita el roaming de datos y voz. |

## La siguiente tabla contiene los comandos disponibles para dispositivos KES.

Comandos disponibles para la administración de dispositivos móviles: dispositivos KES

| Comando | Resultado del comando |
|---|---|
| Bloquear | El dispositivo móvil se bloquea. |
| Desbloquear | Se deshabilita el bloqueo del dispositivo móvil con código PIN. Se elimina el código PIN configurado. |
| Restablecer ajustes de fábrica | Se eliminan todos los datos del dispositivo móvil y se restaura la configuración de fábrica. |
| Eliminar datos corporativos | Se eliminan los datos corporativos, las entradas de la lista de contactos, el historial de mensajes SMS, el registro de llamadas, el calendario, los ajustes de conexión a Internet y las cuentas de usuario (excepto la cuenta de Google). Se borran los datos de la tarjeta de memoria. |
| Sincronizar dispositivo | Los datos del dispositivo móvil se sincronizan con el Servidor de administración. |
| Localizar dispositivo | Se localiza el dispositivo móvil y se muestra su ubicación en Google Maps™. El operador de servicios móviles aplica un cargo por enviar mensajes de texto y por proporcionar la conexión a Internet. |
| Foto de identificación | El dispositivo móvil se bloquea. Se toma una foto con la cámara frontal del dispositivo y se la guarda en el Servidor de administración. Estas fotos se pueden ver en el registro de comandos. El operador de servicios móviles aplica un cargo por enviar mensajes de texto y por proporcionar la conexión a Internet. |
| Alarma | Suena una alarma en el dispositivo móvil. |

## Usar Firebase Cloud Messaging

Para asegurar la distribución a tiempo de los comandos a los dispositivos KES administrados por el sistema operativo Android, Kaspersky Security Center utiliza el mecanismo de notificaciones push. Las notificaciones push se intercambian entre los dispositivos KES y el Servidor de administración a través de Firebase Cloud Messaging (en adelante, FCM). En la Consola de administración de Kaspersky Security Center, puede especificar la configuración de Firebase Cloud Messaging para conectar los dispositivos KES al servicio.

Para recuperar la configuración de Firebase Cloud Messaging, debe tener una cuenta de Google.

*Para habilitar el uso de FCM:*

1. En la Consola de administración, seleccione el nodo **Administración de dispositivos móviles** y la carpeta **Dispositivos móviles**.
2. En el menú contextual de la carpeta **Dispositivos móviles**, seleccione **Propiedades**.
3. En las propiedades de la carpeta, seleccione la sección **Configuración de Firebase Cloud Messaging**.
4. En el campo **Número de proyecto de Firebase**, especifique el Id. del remitente de FCM.
5. En el campo **Archivo de clave privada (en formato JSON)**, seleccione el archivo de clave privada.

   En la próxima sincronización con el Servidor de administración, los dispositivos KES administrados por sistemas operativos Android estarán conectados a Firebase Cloud Messaging.

Puede editar la configuración de Firebase Cloud Messaging al hacer clic en el botón **Restablecer configuración**.

## Enviar comandos

*Para enviar un comando al dispositivo móvil del usuario:*

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.
2. Seleccione el dispositivo móvil del usuario al que necesita enviar un comando.
3. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

4. En la ventana **Comandos para la administración de dispositivos móviles** vaya a la sección con el nombre del comando que necesita enviar al dispositivo móvil, luego haga clic en el botón **Enviar comando**.

   Según el comando que haya seleccionado, haga clic en el botón **Enviar comando** para abrir la ventana de configuración avanzada de la aplicación. Por ejemplo, cuando envía el comando para eliminar un perfil de aprovisionamiento de un dispositivo móvil, la aplicación le solicita que seleccione el perfil de aprovisionamiento que debe eliminarse del dispositivo móvil. Defina la configuración avanzada del comando en esa ventana y confirme su selección. Después de esto, el comando se enviará al dispositivo móvil.

   Puede hacer clic en el botón **Reenviar** para enviar nuevamente el comando al dispositivo móvil del usuario.

   Puede hacer clic en el botón **Eliminar de la cola** para cancelar la ejecución de un comando enviado si este aún no se ha ejecutado.

   La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo móvil, con los respectivos estados de ejecución. Haga clic en **Actualizar** para actualizar la lista de comandos.

5. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para la administración de dispositivos móviles**.

## Ver los estados de los comandos en el registro de comandos

La aplicación guarda en el registro de comandos la información acerca de todos los comandos que se han enviado a los dispositivos móviles. El registro de comandos contiene información acerca de la fecha y hora en que se envió cada comando al dispositivo móvil, sus respectivos estados y las descripciones detalladas de los resultados de ejecución del comando. Por ejemplo, en el caso de que la ejecución de un comando no se realice con éxito, el registro muestra la causa del error. Los registros se almacenan en el registro de comandos por 30 días como máximo.

Los comandos enviados a los dispositivos móviles pueden tener los siguientes estados:

- *En ejecución*: El comando se envió al dispositivo móvil.
- *Completado*: la ejecución del comando ha finalizado exitosamente.
- *Completado con error*: La ejecución del comando falló.
- *Eliminando*: el comando se está eliminando de la cola de comandos enviados al dispositivo móvil.
- *Eliminado*: El comando se ha eliminado correctamente de la cola de comandos enviados al dispositivo móvil.
- *Error al eliminar:* el comando no se pudo eliminar de la cola de comandos enviados al dispositivo móvil.

La aplicación mantiene un registro de comandos para cada dispositivo móvil.

*Para ver el registro de comandos enviados a un dispositivo móvil:*

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En la lista de dispositivos móviles, seleccione aquel para el que desee ver el registro de comandos.

3. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

   Se abre la ventana **Comandos para la administración de dispositivos móviles**. Las secciones de la ventana **Comandos para la administración de dispositivos móviles** corresponden a los comandos que pueden enviarse al dispositivo móvil.

4. Seleccione las secciones que contengan los comandos que necesita y vea información acerca de cómo se envían y ejecutan los comandos al abrir la sección **Registro de comandos**.

En la sección **Registro de comandos**, puede ver la lista de comandos que se han enviado al dispositivo móvil y detalles sobre esos comandos. El filtro **Mostrar comandos** le permite mostrar en la lista solo los comandos con el estado seleccionado.

# Trabajar con certificados de dispositivos móviles

Esta sección brinda información sobre cómo trabajar con certificados de dispositivos móviles.

El certificado raíz para dispositivos móviles tiene un plazo de caducidad fijo de 700 días después de su generación. El certificado de reserva se genera 60 días antes de la fecha de caducidad. Puede modificar el período para generar un certificado de reserva con el siguiente comando:

`klscflag.exe -fset -pv klserver -n KLSRV_AKLWNGT_MDM_CERT_CHANGE_TIMEOUT -t d -v <tiempo de espera en segundos>`

El período para generar un certificado de reserva debe ser lo suficientemente extenso para que todos los dispositivos móviles administrados se sincronicen con el Servidor de administración y recuperen el certificado.

La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada es <Disk>:\Archivos de programa(x86)\Kaspersky Lab\Kaspersky Security Center.

No se admite la renovación manual del certificado raíz para dispositivos móviles.

## Iniciar el Asistente de instalación de certificados

Puede instalar los siguientes tipos de certificados en el dispositivo móvil de un usuario:

- Certificados compartidos para identificar el dispositivo móvil
- Certificados de correo para configurar el correo corporativo en el dispositivo móvil
- Certificado de VPN para configurar el acceso a una red privada virtual en el dispositivo móvil

*Para instalar un certificado en el dispositivo móvil de un usuario:*

1. En el árbol de consola, expanda la carpeta **Administración de dispositivos móviles** y seleccione la subcarpeta **Certificados**.

2. En el espacio de trabajo de la carpeta **Certificados**, haga clic en el vínculo **Agregar certificado** para ejecutar el Asistente de instalación de certificados.

Siga las instrucciones del asistente.

Una vez que finalice el Asistente, se creará un certificado y se agregará a la lista de certificados del usuario; además al usuario se le enviará una notificación con un vínculo para descargar e instalar el certificado en el dispositivo móvil. Puede ver la lista de todos los certificados y exportarla a un archivo. Puede eliminar o volver a emitir certificados, así como ver sus propiedades.

## Paso 1. Selección del tipo de certificado

Especifique el tipo de certificado que debe instalarse en el dispositivo móvil del usuario:

- **Certificado para dispositivos móviles**: para identificar el dispositivo móvil
- **Certificado de correo**: para configurar el correo corporativo en el dispositivo móvil
- **Certificado de VPN**: para configurar el acceso a una red privada virtual en el dispositivo móvil

## Paso 2. Selección del tipo de dispositivo

Esta ventana se muestra solo si seleccionó **Certificado de correo** o **Certificado de VPN** como el tipo de certificado.

Especifique el tipo de sistema operativo en el dispositivo:

- **Dispositivo MDM con iOS**. Seleccione esta opción si tiene que instalar un certificado en un dispositivo móvil que está conectado al servidor de MDM para iOS utilizando el protocolo MDM para iOS.
- **Dispositivo KES administrado mediante Kaspersky Security para dispositivos móviles**. Seleccione esta opción si tiene que instalar un certificado en un dispositivo KES. En este caso, el certificado se usará para la identificación del usuario en cada conexión al Servidor de administración.
- **Dispositivo KES conectado al Servidor de administración sin autenticarse mediante certificado de usuario**. Seleccione esta opción si tiene que instalar un certificado en un dispositivo KES sin autenticación de certificado. En este caso, en el paso final del Asistente, en la ventana **Método de notificación al usuario**, el administrador debe seleccionar el tipo de autenticación de usuario utilizado en cada conexión al Servidor de administración.

## Paso 3. Selección de un usuario

En la lista, seleccione usuarios, grupos de seguridad o grupos de seguridad de Active Directory para los cuales debe instalar el certificado.

En la ventana **Selección de usuario**, puede buscar usuarios internos de Kaspersky Security Center. Puede hacer clic en **Agregar** para añadir a un usuario interno.

## Paso 4. Selección del origen del certificado

En esta ventana, puede seleccionar el origen del certificado que usará el Servidor de administración para identificar el dispositivo móvil. Puede especificar un certificado usando uno de los siguientes métodos:

- Crear un certificado automáticamente (con las herramientas del Servidor de administración) y luego entregarlo al dispositivo.

- Especificar un archivo de certificado que se creó antes. Este método no está disponible si se seleccionaron varios usuarios en el paso anterior.

Seleccione la casilla de verificación **Publicar certificado** si debe enviar a un usuario una notificación sobre la creación de un certificado para su dispositivo móvil.

Si el dispositivo móvil del usuario ya se ha autenticado previamente con un certificado, por lo que no es necesario especificar un nombre de cuenta y una contraseña para recibir un certificado nuevo, desactive la casilla de verificación **Publicar certificado**. En este caso, no aparecerá la ventana **Método de notificación al usuario**.

## Paso 5. Asignación de una etiqueta al certificado

Se muestra la ventana **Etiqueta del certificado** si se ha seleccionado **Dispositivo MDM con iOS** en **Tipo de dispositivo**.

En la lista desplegable, puede asignar una etiqueta al certificado del dispositivo MDM con iOS del usuario. El certificado con la etiqueta asignada puede tener parámetros específicos establecidos para esta etiqueta en las propiedades de directiva de Kaspersky Device Management for iOS.

La lista desplegable solicita que seleccione la etiqueta *Plantilla de certificado 1*, *Plantilla de certificado 2* o *Plantilla de certificado 3*. Puede configurar las etiquetas en las siguientes secciones:

- Si se ha seleccionado **Certificado de correo** en la ventana **Tipo de certificado**, las etiquetas respectivas se pueden configurar en las propiedades de la cuenta de Exchange ActiveSync para dispositivos móviles (**Dispositivos administrados** → **Directivas** → Propiedades de directiva de Kaspersky Device Management for iOS → **Exchange ActiveSync** sección → **Agregar** → **Avanzado**).

- Si se ha seleccionado **Certificado de VPN** en la ventana **Tipo de certificado**, las etiquetas respectivas se pueden configurar en las propiedades de la VPN para dispositivos móviles (**Dispositivos administrados** → **Directivas** → Propiedades de directiva de Kaspersky Device Management for iOS → **VPN** sección → **Agregar** → **Avanzado**). No puede configurar las etiquetas utilizadas para los certificados de VPN si selecciona el tipo de conexión L2TP, PPTP o IPSec (Cisco™) para su VPN.

## Paso 6. Especificación de configuración de publicación de certificados

En esta ventana, puede especificar la siguiente configuración de publicación de certificados:

- **No informar al usuario sobre un nuevo certificado**

  Active esta opción si no desea enviar a un usuario una notificación de la creación de un certificado para el dispositivo móvil del usuario. En este caso, no aparecerá la ventana **Método de notificación al usuario**.

  Esta opción solo se aplica a dispositivos con Kaspersky Endpoint Security para Android instalado.

  Es posible que desee activar esta opción, por ejemplo, si el dispositivo móvil del usuario ya se ha autenticado previamente mediante un certificado, por lo que no es necesario especificar un nombre de cuenta y una contraseña para recibir un nuevo certificado.

- **Permitir que el dispositivo tenga varios recibos de un mismo certificado (solo para dispositivos con Kaspersky Endpoint Security para Android instalado)**

  Active esta opción si desea que Kaspersky Security Center reenvíe automáticamente el certificado cada vez que caduque o cuando no se encuentre en el dispositivo de destino.

  El certificado se reenvía automáticamente varios días antes de la fecha de caducidad del certificado. Puede establecer el número de días en la ventana Reglas de emisión de certificados.

  En algunos casos, el certificado no se puede encontrar en el dispositivo. Por ejemplo, esto puede pasar cuando el usuario instala de nuevo la aplicación de seguridad de Kaspersky en el dispositivo o reinicializa la configuración del dispositivo y datos a faltas de la fábrica. En este caso, Kaspersky Security Center verifica la identificación del dispositivo en el siguiente intento del dispositivo para conectarse al Servidor de administración. Si el dispositivo tiene el mismo id. que tenía cuando se emitió el certificado, la aplicación reenvía el certificado al dispositivo.

## Paso 7. Selección del método de notificación al usuario

Esta ventana no se muestra si seleccionó **Dispositivo MDM con iOS** como el tipo de dispositivo o si seleccionó la opción **No informar al usuario sobre un nuevo certificado**.

En la ventana **Método de notificación al usuario**, puede configurar la notificación al usuario acerca de la instalación del certificado en el dispositivo móvil.

En el campo **Método de autenticación**, especifique el tipo de autenticación de usuario:

- **Credenciales (dominio o alias)**

  En este caso, el usuario emplea la contraseña de dominio o la contraseña de un usuario interno de Kaspersky Security Center para recibir un nuevo certificado.

- **Contraseña de un solo uso**

  En este caso, el usuario recibe una contraseña de un solo uso que se enviará por correo electrónico o por SMS. Debe ingresarse esta contraseña para recibir un nuevo certificado.

  Esta opción cambia a **Contraseña** si activó (seleccionó) la opción **Permitir que el dispositivo reciba múltiples recibos de un solo certificado (solo para dispositivos con aplicaciones de seguridad Kaspersky para dispositivos móviles instalados)** en la ventana **Opciones para la publicación del certificado**.

- **Contraseña**

  En este caso, la contraseña se utiliza cada vez que el certificado se envía al usuario.

  Esta opción cambia a **Contraseña de un solo uso** si desactivó (deseleccionó) la opción **Permitir que el dispositivo reciba múltiples recibos de un solo certificado (solo para dispositivos con aplicaciones de seguridad Kaspersky para dispositivos móviles instalados)** en la ventana **Opciones para la publicación del certificado**.

Este campo se muestra si seleccionó **Certificado para dispositivos móviles** en la ventana **Tipo de certificado** o si seleccionó **Dispositivo KES conectado al Servidor de administración sin autenticarse mediante certificado de usuario** como tipo de dispositivo.

Seleccione la opción de notificación de usuario:

- **Mostrar la contraseña de autenticación cuando finalice el asistente**

  Si selecciona esta opción, el nombre de usuario, el nombre de usuario en el Administrador de cuentas de seguridad (SAM) y la contraseña para la recuperación de certificados para cada uno de los usuarios seleccionados se mostrarán en el paso final del Asistente de instalación de certificados. La configuración de la notificación del usuario sobre un certificado instalado no estará disponible.

  Cuando agrega certificados para varios usuarios, puede guardar las credenciales proporcionadas en un archivo haciendo clic en el botón **Exportar** en el último paso del Asistente de instalación de certificados.

  Esta opción no está disponible si seleccionó **Credenciales (dominio o alias)** en el paso **Método de notificación del usuario** del Asistente de instalación de certificados.

- **Informar al usuario sobre el nuevo certificado**

  Si selecciona esta opción, puede configurar la notificación del usuario sobre un nuevo certificado.

  - **Por correo electrónico**

    En este grupo de configuración Por correo electrónico, puede configurar notificaciones de usuario sobre la instalación de un nuevo certificado en su dispositivo móvil mediante mensajes de correo electrónico. Este método de notificación solo está disponible si el Servidor SMTP está habilitado.

    Haga clic en el enlace **Editar mensaje** para ver y editar el mensaje de notificación, si es necesario.

  - **Por SMS**

    En este grupo de configuraciones, puede configurar la notificación del usuario sobre el uso de SMS para instalar un certificado en dispositivos móviles. Este método de notificación solo está disponible si Notificación por SMS está habilitada.

    Haga clic en el enlace **Editar mensaje** para ver y editar el mensaje de notificación, si es necesario.

### Paso 8. Generación del certificado

En este paso se crea el certificado.

Puede hacer clic en **Finalizar** para salir del asistente.

El certificado se genera y se muestra en la lista de certificados en el espacio de trabajo de la carpeta **Certificados**.

## Configuración de las reglas de emisión de certificados

Los certificados se utilizan para la autenticación del dispositivo en el Servidor de administración. Todos los dispositivos móviles administrados deben tener certificados. Puede configurar cómo se emiten los certificados.

*Para configurar las reglas de emisión de certificados:*

1. En el árbol de consola, expanda la carpeta **Administración de dispositivos móviles** y seleccione la subcarpeta **Certificados**.

2. En el espacio de trabajo de la carpeta **Certificados**, haga clic en el botón **Configurar reglas de emisión de certificados** para abrir la ventana **Reglas de emisión de certificados**.

3. Vaya a la sección con el nombre de un tipo de certificado:

   **Emisión de certificados para dispositivos móviles**: para configurar la emisión de certificados para los dispositivos móviles.

   **Emisión de certificados de correo**: para configurar la emisión de certificados de correo.

   **Emisión de certificados de VPN**: para configurar la emisión de certificados de VPN.

4. En la sección **Configuración de emisión**, configure la emisión del certificado:

   - Especifique la duración del certificado en días.

     Los certificados para dispositivos móviles están limitados por la fecha de caducidad del certificado raíz. Si especifica un plazo más extenso del certificado que la fecha de caducidad del certificado raíz, el plazo del certificado se ajustará automáticamente al generarlo.

   - Seleccione una fuente de certificado (**Servidor de administración** o **Los certificados se especifican manualmente**).

     El Servidor de administración está seleccionado como la fuente predeterminada de los certificados.

   - Especifique una plantilla de certificado (**Plantilla predeterminada**, **Otra plantilla**).

     La configuración de plantillas está disponible si la sección **Integración con PKI** cuenta con la integración con la infraestructura de claves públicas habilitada.

5. En la sección **Configuración de actualización automática** configure las actualizaciones automáticas del certificado:

   - En el campo **Renovar cuando el certificado caduque en (días)**, especifique cuántos días antes del vencimiento se debe renovar el certificado.

   - Para habilitar las actualizaciones automáticas de certificados, seleccione la casilla de verificación **Volver a emitir certificados automáticamente si es posible**.

6. En la sección **Protección con contraseña**, habilite y configure el uso de una contraseña para descifrar certificados.

   La protección con contraseña solo está disponible para certificados de celular.

   a. Seleccione la casilla **Solicitar contraseña durante la instalación de certificados**.

   b. Use el control deslizante para definir el número máximo de símbolos en la contraseña para cifrado.

7. Haga clic en **Aceptar**.

## Integración con la infraestructura de claves públicas

Para simplificar la emisión de certificados de dominio para los usuarios, se requiere la integración de la aplicación con la Infraestructura de claves públicas (PKI). Una vez que se completa la integración, los certificados se emiten automáticamente.

La versión del servidor de PKI admitida mínima es Windows Server 2008.

Debe configurar la cuenta para la integración con PKI. La cuenta debe reunir los siguientes requisitos:

- Ser un usuario de dominio y administrador del dispositivo en el que se encuentra instalado el Servidor de administración.
- Tener el privilegio SeServiceLogonRight en el dispositivo que aloja al Servidor de administración.

Para crear un perfil de usuario permanente ingrese al menos una vez bajo la cuenta de usuario configurada en el dispositivo donde está instalado el Servidor de administración. En el repositorio de certificados de este usuario, en el dispositivo donde se encuentra el Servidor de administración, instale el certificado de agente de inscripción provisto por los administradores del dominio.

*Para configurar la integración con la infraestructura de claves públicas:*

1. En el árbol de consola, expanda la carpeta **Administración de dispositivos móviles** y seleccione la subcarpeta **Certificados**.
2. En el espacio de trabajo, haga clic en el botón **Integrar con infraestructura de claves públicas** para abrir la sección **Integración con PKI** de la ventana **Reglas de emisión de certificados**.

   La sección **Integración con PKI** de la ventana **Reglas de emisión de certificados** se abre.
3. Seleccione la casilla **Integrar la emisión de certificados con PKI**.
4. En el campo **Cuenta** especifique el nombre de la cuenta de usuario que se usará para la integración con la infraestructura de claves públicas.
5. En el campo **Contraseña** ingrese la contraseña de dominio para la cuenta.
6. En la lista **El nombre de la plantilla de certificado en el sistema PKI**, seleccione la plantilla del certificado que se utilizará para la emisión de certificados de usuarios de dominio.

   En Kaspersky Security Center se ejecuta un servicio dedicado bajo la cuenta de usuario especificada. Este servicio es responsable de emitir los certificados de dominio de los usuarios. El servicio inicia cuando se carga la lista de plantillas de certificados haciendo clic en el botón **Actualizar lista** o cuando se genera un certificado.
7. Haga clic en **Aceptar** para guardar los ajustes.

Una vez que se completa la integración, los certificados se emiten automáticamente.

## Habilitar la compatibilidad con la delegación restringida de Kerberos

La aplicación admite el uso de la delegación restringida de Kerberos.

*Para habilitar el uso de la delegación restringida de Kerberos:*

1. En el árbol de la consola, abra la carpeta **Administración de dispositivos móviles**.
2. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Servidores de dispositivos móviles**.
3. En el espacio de trabajo de la carpeta **Servidores de dispositivos móviles**, seleccione un Servidor de MDM para iOS.
4. En el menú contextual del Servidor de MDM para iOS, seleccione **Propiedades**.
5. En la ventana de propiedades del Servidor de MDM para iOS, seleccione la sección **Configuración**.
6. En la sección **Configuración**, seleccione la casilla de verificación **Asegurar compatibilidad con la delegación restringida de Kerberos**.
7. Haga clic en **Aceptar**.

## Adición de dispositivos móviles iOS a la lista de dispositivos administrados

Para agregar un dispositivo móvil iOS a la lista de dispositivos administrados, debe entregarse e instalarse un certificado compartido en el dispositivo. Los certificados compartidos son utilizados por el Servidor de administración para identificar dispositivos móviles. El certificado compartido para un dispositivo móvil iOS se entrega dentro de un perfil de MDM para iOS. Una vez que se entrega e instala un certificado compartido en un dispositivo móvil, este aparece en la lista de dispositivos administrados.

Kaspersky ha discontinuado Kaspersky Safe Browser.

Puede agregar dispositivos móviles de usuarios a la lista de dispositivos administrados mediante el Asistente para conectar un nuevo dispositivo móvil.

*Para conectar un dispositivo iOS al Servidor de administración mediante un certificado compartido, haga lo siguiente:*

1. Inicie el Asistente para conectar un nuevo dispositivo móvil de una de las siguientes maneras:

   - Use el menú contextual en la carpeta **Cuentas de usuario**:

     1. En el árbol de consola, expanda la carpeta **Avanzado** y seleccione la subcarpeta **Cuentas de usuario**.

     2. En el espacio de trabajo de la carpeta **Cuentas de usuario**, seleccione a los usuarios, grupos de seguridad o grupos de seguridad de Active Directory cuyos dispositivos móviles desea agregar a la lista de dispositivos administrados.

     3. Haga clic derecho y en el menú contextual de la cuenta de usuario, seleccione **Agregar dispositivo móvil**.

        El Asistente para conectar un nuevo dispositivo móvil empieza a ejecutarse.

   - En el espacio de trabajo de la carpeta **Dispositivos móviles**, haga clic en el botón **Agregar dispositivo móvil**:

     1. En el árbol de la consola, expanda la carpeta **Administración de dispositivos móviles** y seleccione la subcarpeta **Dispositivos móviles**.

     2. En el espacio de trabajo de esta subcarpeta **Dispositivos móviles**, haga clic en el botón **Agregar dispositivo móvil**.

        El Asistente para conectar un nuevo dispositivo móvil empieza a ejecutarse.

2. En la página del Asistente **Sistema operativo**, seleccione **iOS** como tipo de sistema operativo del dispositivo móvil.

3. En la página **Seleccione un Servidor de MDM para iOS**, seleccione el Servidor de MDM para iOS.

4. En la página **Seleccione a los usuarios de los dispositivos móviles que administrará**, seleccione a los usuarios, grupos de seguridad o grupos de seguridad de Active Directory cuyos dispositivos móviles desea agregar a la lista de dispositivos administrados.

   Este paso se omite si inicia el Asistente al seleccionar **Agregar dispositivo móvil** en el menú contextual de la carpeta **Cuentas de usuario**.

   Si desea agregar una nueva cuenta de usuario a la lista, haga clic en el botón **Agregar** e introduzca las propiedades de la cuenta de usuario en la ventana que se abre. Si desea modificar o revisar las propiedades de la cuenta de usuario, seleccione la cuenta de usuario en la lista y haga clic en el botón **Propiedades**.

5. En la página del asistente **Origen del certificado**, especifique el método de creación del certificado compartido que utilizará el Servidor de administración para identificar el dispositivo móvil. Puede especificar un certificado compartido usando uno de los siguientes métodos:

   - **Emitir certificado usando las herramientas del Servidor de administración**

     Seleccione esta opción para crear un nuevo certificado con las herramientas del Servidor de administración si todavía no lo ha creado.

     Si esta opción se selecciona, el perfil de MDM para iOS se firmará con un certificado generado automáticamente mediante el Servidor de administración.

     Esta opción está seleccionada de forma predeterminada.

   - **Especificar archivo de certificado**

     Seleccione esta opción para especificar un archivo de certificado que ya se ha creado.

     Este método no está disponible si se seleccionaron varios usuarios en el paso anterior.

6. En la página **Método de notificación al usuario** del asistente, defina la configuración para notificar al usuario del dispositivo móvil por SMS o correo electrónico sobre la creación del certificado:

   - **Mostrar código QR en el asistente**

     Si selecciona esta opción, se mostrará un enlace al paquete de instalación en el paso final del Asistente para conectar un nuevo dispositivo móvil.

     Esta opción no está disponible si se seleccionaron varios usuarios para la conexión del dispositivo.

   - **Enviar código QR al usuario**

     Seleccionar esta opción le permite configurar la notificación de usuario de conexión de un dispositivo móvil nuevo.

     Puede seleccionar el tipo de dirección de correo electrónico, especificar una dirección de correo electrónico adicional y modificar el texto del mensaje. También puede seleccionar el tipo del teléfono de usuario para enviar un mensaje de texto, especificar un número de teléfono adicional y modificar el texto del mensaje de texto.

     Si el Servidor SMTP no se ha configurado, no se puede enviar ningún mensaje de correo electrónico a usuarios. Si la notificación de SMS no se ha configurado, no se puede enviar ningún mensaje de correo electrónico a usuarios.

7. En la página **Resultado**, haga clic en **Finalizar** para cerrar el asistente.

El perfil de MDM para iOS se publica automáticamente en el servidor web de Kaspersky Security Center. El usuario del dispositivo móvil recibe una notificación con un enlace para descargar el perfil de MDM para iOS del servidor web. El usuario hace clic en el enlace. A continuación, el sistema operativo del dispositivo móvil le solicita al usuario que acepte la instalación del perfil de MDM para iOS. El usuario debe aceptar instalar el perfil de MDM para iOS antes de que el perfil de MDM para iOS se pueda descargar al dispositivo móvil. Una vez que el perfil de MDM para iOS se descarga y el dispositivo móvil se sincroniza con el Servidor de administración, el dispositivo aparece en la carpeta **Dispositivos móviles**, que es una subcarpeta de la carpeta **Administración de dispositivos móviles** del árbol de consola.

Para que el usuario acceda al servidor web de Kaspersky Security Center mediante el enlace, el dispositivo móvil debe poder conectarse al Servidor de administración a través del puerto 8061.

# Incorporar dispositivos móviles Android a la lista de dispositivos administrados

Para agregar un dispositivo móvil Android a la lista de dispositivos administrados, Kaspersky Endpoint Security para Android y un certificado compartido se deben entregar e instalar en el dispositivo móvil. Los certificados compartidos son utilizados por el Servidor de administración para identificar dispositivos móviles. Una vez que se entrega e instala un certificado compartido en un dispositivo móvil, este aparece en la lista de dispositivos administrados.

Puede agregar dispositivos móviles de usuarios a la lista de dispositivos administrados mediante el Asistente para conectar un nuevo dispositivo móvil. El asistente proporciona dos opciones para entregar e instalar un certificado compartido y Kaspersky Endpoint Security for Android:

- Utilizando el enlace de Google Play
- Utilizando un enlace del servidor web de Kaspersky Security Center

  El paquete de instalación de Kaspersky Endpoint Security para Android almacenado para la distribución en el Servidor de administración se utiliza para la instalación

## Inicio del Asistente para conectar un nuevo dispositivo móvil

*Para iniciar el Asistente para conectar un nuevo dispositivo móvil, realice una de las siguientes acciones:*

- Use el menú contextual en la carpeta **Cuentas de usuario**:

  1. En el árbol de consola, expanda la carpeta **Avanzado** y seleccione la subcarpeta **Cuentas de usuario**.
  2. En el espacio de trabajo de la carpeta **Cuentas de usuario**, seleccione a los usuarios, grupos de seguridad o grupos de seguridad de Active Directory cuyos dispositivos móviles desea agregar a la lista de dispositivos administrados.
  3. Haga clic derecho y en el menú contextual de la cuenta de usuario, seleccione **Agregar dispositivo móvil**.

     El Asistente para conectar un nuevo dispositivo móvil empieza a ejecutarse.

- En el espacio de trabajo de la carpeta **Dispositivos móviles**, haga clic en el botón **Agregar dispositivo móvil**:

  1. En el árbol de la consola, expanda la carpeta **Administración de dispositivos móviles** y seleccione la subcarpeta **Dispositivos móviles**.
  2. En el espacio de trabajo de esta subcarpeta **Dispositivos móviles**, haga clic en el botón **Agregar dispositivo móvil**.

     El Asistente para conectar un nuevo dispositivo móvil empieza a ejecutarse.

## Agregar un dispositivo móvil Android utilizando el enlace de Google Play

*Para instalar Kaspersky Endpoint Security para Android y un certificado compartido en un dispositivo móvil mediante un enlace de Google Play, realice lo siguiente:*

1. Inicie el Asistente para conectar un nuevo dispositivo móvil.
2. En la página del asistente **Sistema operativo**, seleccione **Android** como tipo del sistema operativo del dispositivo móvil.
3. En la página **Método para instalar Kaspersky Endpoint Security for Android en los dispositivos** del asistente, seleccione **Descargar la app desde Google Play**.
4. En la página **Seleccione a los usuarios de los dispositivos móviles que administrará** del Asistente, seleccione a los usuarios, grupos de seguridad o grupos de seguridad de Active Directory cuyos dispositivos móviles desea agregar a la lista de dispositivos administrados.

   Este paso se omite si se inicia el asistente seleccionando **Agregar dispositivo móvil** en el menú contextual de la carpeta **Cuentas de usuario**.

   Si desea agregar una nueva cuenta de usuario a la lista, haga clic en el botón **Agregar** e introduzca las propiedades de la cuenta de usuario en la ventana que se abre. Si desea modificar o revisar las propiedades de la cuenta de usuario, seleccione la cuenta de usuario en la lista y haga clic en el botón **Propiedades**.
5. En la página del asistente **Origen del certificado**, especifique el método de creación del certificado compartido que utilizará el Servidor de administración para identificar el dispositivo móvil. Puede especificar un certificado compartido usando uno de los siguientes métodos:

   - Emitir certificado usando las herramientas del Servidor de administración

     Seleccione esta opción para crear un nuevo certificado con las herramientas del Servidor de administración si todavía no lo ha creado.

     Si selecciona esta opción, el certificado se emite automáticamente por medio de las herramientas del Servidor de administración.

     Esta opción está seleccionada de forma predeterminada.

   - Especificar archivo de certificado

     Seleccione esta opción para especificar un archivo de certificado que ya se ha creado.

     Este método no está disponible si se seleccionaron varios usuarios en el paso anterior.

6. En la página **Método de notificación al usuario** del asistente, defina la configuración para notificar al usuario del dispositivo móvil por SMS o correo electrónico sobre la creación del certificado:

   - Mostrar código QR en el asistente

     Si selecciona esta opción, se mostrará un enlace al paquete de instalación en el paso final del Asistente para conectar un nuevo dispositivo móvil.

     Esta opción no está disponible si se seleccionaron varios usuarios para la conexión del dispositivo.

   - Enviar código QR al usuario

     Seleccionar esta opción le permite configurar la notificación de usuario de conexión de un dispositivo móvil nuevo.

     Puede seleccionar el tipo de dirección de correo electrónico, especificar una dirección de correo electrónico adicional y modificar el texto del mensaje. También puede seleccionar el tipo del teléfono de usuario para enviar un mensaje de texto, especificar un número de teléfono adicional y modificar el texto del mensaje de texto.

     Si el Servidor SMTP no se ha configurado, no se puede enviar ningún mensaje de correo electrónico a usuarios. Si la notificación de SMS no se ha configurado, no se puede enviar ningún mensaje de correo electrónico a usuarios.

7. En la página **Resultado**, haga clic en **Finalizar** para cerrar el asistente.

Cuando el asistente finaliza, el usuario recibe en el dispositivo móvil un enlace y un código QR para descargar Kaspersky Endpoint Security para Android. El usuario hace clic en el enlace o escanea el código QR. A continuación, el sistema operativo del dispositivo móvil le solicita al usuario que acepte la instalación de Kaspersky Endpoint Security para Android. Al concluir la descarga e instalación de Kaspersky Endpoint Security para Android, el dispositivo móvil se conecta con el Servidor de administración y descarga un certificado compartido. Una vez que el certificado se instala en el dispositivo móvil, el dispositivo aparece en la carpeta **Dispositivos móviles**, que es una subcarpeta de la carpeta **Administración de dispositivos móviles** en el árbol de consola.

## Agregar un dispositivo móvil Android utilizando un enlace del servidor web de Kaspersky Security Center

Para la instalación, se utiliza el paquete de instalación de Kaspersky Endpoint Security para Android publicado en el Servidor de administración.

*Para instalar Kaspersky Endpoint Security para Android y un certificado compartido en un dispositivo móvil utilizando un enlace del servidor web, realice lo siguiente:*

1. Inicie el Asistente para conectar un nuevo dispositivo móvil.

2. En la página del asistente **Sistema operativo**, seleccione **Android** como tipo del sistema operativo del dispositivo móvil.

3. En la página del **Método para instalar Kaspersky Endpoint Security for Android en los dispositivos** del Asistente, seleccione **Descargar el paquete de instalación desde Kaspersky Security Center**.

   En el campo que aparece a continuación, seleccione un paquete de instalación o cree uno nuevo al hacer clic en **Nuevo**.

4. En la página **Seleccione a los usuarios de los dispositivos móviles que administrará** del Asistente, seleccione a los usuarios, grupos de seguridad o grupos de seguridad de Active Directory cuyos dispositivos móviles desea agregar a la lista de dispositivos administrados.

   > Este paso se omite si se inicia el asistente seleccionando **Agregar dispositivo móvil** en el menú contextual de la carpeta **Cuentas de usuario**.

   Si desea agregar una nueva cuenta de usuario a la lista, haga clic en el botón **Agregar** e introduzca las propiedades de la cuenta de usuario en la ventana que se abre. Si desea modificar o revisar las propiedades de la cuenta de usuario, seleccione la cuenta de usuario en la lista y haga clic en el botón **Propiedades**.

5. En la página del asistente **Origen del certificado**, especifique el método de creación del certificado compartido que utilizará el Servidor de administración para identificar el dispositivo móvil. Puede especificar un certificado compartido usando uno de los siguientes métodos:

   - Emitir certificado usando las herramientas del Servidor de administración

     > Seleccione esta opción para crear un nuevo certificado con las herramientas del Servidor de administración si todavía no lo ha creado.
     >
     > Si selecciona esta opción, el certificado se emite automáticamente por medio de las herramientas del Servidor de administración.
     >
     > Esta opción está seleccionada de forma predeterminada.

   - Especificar archivo de certificado

     > Seleccione esta opción para especificar un archivo de certificado que ya se ha creado.
     >
     > Este método no está disponible si se seleccionaron varios usuarios en el paso anterior.

6. En la página **Método de notificación al usuario** del asistente, defina la configuración para notificar al usuario del dispositivo móvil por SMS o correo electrónico sobre la creación del certificado:

   - Mostrar código QR en el asistente

     Si selecciona esta opción, se mostrará un enlace al paquete de instalación en el paso final del Asistente para conectar un nuevo dispositivo móvil.

     Esta opción no está disponible si se seleccionaron varios usuarios para la conexión del dispositivo.

   - Enviar código QR al usuario

     Seleccionar esta opción le permite configurar la notificación de usuario de conexión de un dispositivo móvil nuevo.

     Puede seleccionar el tipo de dirección de correo electrónico, especificar una dirección de correo electrónico adicional y modificar el texto del mensaje. También puede seleccionar el tipo del teléfono de usuario para enviar un mensaje de texto, especificar un número de teléfono adicional y modificar el texto del mensaje de texto.

     Si el Servidor SMTP no se ha configurado, no se puede enviar ningún mensaje de correo electrónico a usuarios. Si la notificación de SMS no se ha configurado, no se puede enviar ningún mensaje de correo electrónico a usuarios.

7. En la página **Resultado**, haga clic en **Finalizar** para cerrar el asistente.

El paquete de aplicaciones móviles de Kaspersky Endpoint Security para Android se publica automáticamente en el servidor web de Kaspersky Security Center. El paquete de aplicaciones móviles contiene la app, los valores de configuración para que el dispositivo móvil se conecte al Servidor de administración y un certificado. El usuario del dispositivo móvil recibe una notificación con un enlace para descargar el paquete del servidor web. El usuario hace clic en el enlace. A continuación, el sistema operativo del dispositivo solicita al usuario que acepte la instalación del paquete de aplicaciones móviles. Si el usuario acepta, el paquete se descargará al dispositivo móvil. Una vez que el paquete se descarga y el dispositivo móvil se sincroniza con el Servidor de administración, el dispositivo aparece en la carpeta **Dispositivos móviles**, que es una subcarpeta de la carpeta **Administración de dispositivos móviles** del árbol de consola.

## Administración de dispositivos MDM con iOS

Esta sección describe las características avanzadas para el manejo de dispositivos MDM con iOS a través de Kaspersky Security Center. La aplicación admite las siguientes funciones para la administración de dispositivos MDM con iOS:

- Definir de modo centralizado los ajustes de los dispositivos MDM con iOS administrados y restringir sus características por medio de perfiles de configuración. Puede agregar o modificar los perfiles de configuración e instalarlos en dispositivos móviles.

- Instalar aplicaciones en dispositivos móviles por medio de perfiles de aprovisionamiento, omitiendo App Store. Por ejemplo, puede usar perfiles de aprovisionamiento para instalar aplicaciones corporativas internas en los dispositivos móviles del usuario. Un perfil de aprovisionamiento contiene información acerca de una app y un dispositivo móvil.

- Instalar aplicaciones en un dispositivo MDM con iOS a través de App Store. Antes de instalar una app en un dispositivo MDM con iOS, debe agregar esa app en un Servidor de MDM para iOS.

Cada 24 horas se envía una notificación push a todos los dispositivos MDM con iOS conectados a fin de sincronizar los datos con el Servidor de MDM para iOS.

Para obtener información acerca del perfil de configuración y el perfil de aprovisionamiento, así como de las aplicaciones instaladas en un dispositivo MDM con iOS, consulte la ventana de propiedades del dispositivo.

## Firmar un perfil de MDM para iOS mediante un certificado

Puede firmar un perfil de MDM para iOS mediante un certificado. Puede utilizar un certificado que haya emitido o puede recibir un certificado de las autoridades de certificación de confianza.

Los dispositivos iOS muestran un descargo de responsabilidad para los perfiles sin firma y solicitan al usuario que confíe en el firmante al instalar el perfil.

*Para firmar un perfil de MDM para iOS mediante un certificado:*

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.
2. En el menú contextual de la carpeta **Dispositivos móviles**, seleccione **Propiedades**.
3. En la ventana de propiedades de la carpeta, seleccione la sección **Opciones de conexión para dispositivos iOS**.
4. Haga clic en el botón **Examinar** debajo del campo **Seleccionar archivo de certificado**.

   La ventana **Certificado**.
5. En el campo **Tipo de certificado**, especifique el tipo de certificado público o privado:
   - Si está seleccionado el valor **Contenedor PKCS #12**, especifique el archivo de certificado y la contraseña.
   - Si está seleccionado el valor **Certificado X.509**:
     a. Especifique el archivo de clave privada (con las extensiones *.prk o *.pem).
     b. Especifique la contraseña de la clave privada.
     c. Especifique el archivo de clave pública (con la extensión *.cer).
6. Haga clic en **Aceptar**.

Un certificado firma el perfil de MDM para iOS.

## Agregar un perfil de configuración

Para crear un perfil de configuración, puede utilizar Apple Configurator 2, que está disponible en el sitio web de Apple Inc. Apple Configurator 2 solo funciona en dispositivos que ejecutan macOS; si no tiene dichos dispositivos a su disposición, puede usar la Utilidad Configuración iPhone en el dispositivo con la Consola de administración. Sin embargo, Apple Inc. ya no admite la Utilidad Configuración iPhone.

*Para crear un perfil de configuración a través de la Utilidad Configuración iPhone y agregarlo a un Servidor de MDM para iOS:*

1. En el árbol de la consola, seleccione la carpeta **Administración de dispositivos móviles**.
2. En el espacio de trabajo de la carpeta **Administración de dispositivos móviles**, haga clic en la subcarpeta **Servidores de dispositivos móviles**.
3. En el espacio de trabajo de la carpeta **Servidores de dispositivos móviles**, seleccione un Servidor de MDM para iOS.
4. En el menú contextual del Servidor de MDM para iOS, seleccione **Propiedades**.

   Se abre la ventana de propiedades del servidor de dispositivos móviles.
5. En la ventana de propiedades del Servidor de MDM para iOS, seleccione la sección **Perfiles de configuración**.
6. En la sección **Perfiles de configuración** haga clic en el botón **Crear**.

   Se abre la ventana **Nuevo perfil de configuración**.
7. En la ventana **Nuevo perfil de configuración** especifique el nombre e ID para el perfil.

   El ID del perfil de configuración debe ser único, se debe especificar el valor en el formato DNS inverso, por ejemplo, *com.companyname.identifier*.
8. Haga clic en **Aceptar**.

   La Utilidad Configuración iPhone se inicia si la tiene instalada.
9. Vuelva a configurar el perfil en iPhone Configuration Utility.

   Para conocer una descripción de la configuración de perfiles e instrucciones sobre cómo configurar el perfil, consulte la documentación adjunta con iPhone Configuration Utility.

Después de haber configurado el perfil con iPhone Configuration Utility, el nuevo perfil de configuración se muestra en la sección **Perfiles de configuración** de la ventana Propiedades del Servidor de MDM para iOS.

Puede hacer clic en el botón **Modificar** para modificar el perfil de configuración.

Puede hacer clic en el botón **Importar** para cargar el perfil de configuración a un programa.

Puede hacer clic en el botón **Exportar** para guardar perfil de configuración en un archivo.

El perfil que ha creado debe instalarse en los dispositivos MDM con iOS.

## Instalación de un perfil de configuración en un dispositivo

*Para instalar un perfil de configuración en un dispositivo móvil:*

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.
2. En el espacio de trabajo, filtre los dispositivos MDM con iOS por protocolo (*MDM para iOS*).

3. Seleccione el dispositivo móvil del usuario en el que debe instalar un perfil de configuración.

   Puede seleccionar múltiples dispositivos móviles para instalar el perfil simultáneamente.

4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

5. En la ventana **Comandos para la administración de dispositivos móviles** vaya a la sección **Instalar perfil** y haga clic en el botón **Enviar comando**.

   También puede enviar el comando al dispositivo móvil seleccionando **Todos los comandos** del menú contextual del dispositivo móvil y después **Instalar perfil**.

   Como resultado, se abre la ventana **Seleccionar perfiles** que muestra una lista de perfiles. Seleccione de la lista el perfil que necesita instalar en el dispositivo móvil. Puede seleccionar múltiples perfiles para instalarlos simultáneamente en el dispositivo móvil. Para seleccionar el rango de perfiles, use la tecla **Mayús**. Para combinar perfiles en un grupo, use la tecla **CTRL**.

6. Haga clic en el botón **Aceptar** para enviar el comando al dispositivo móvil.

   Cuando el comando se ejecute, el perfil de configuración seleccionado se instalará en el dispositivo móvil del usuario. Si el comando se ejecuta correctamente, el estado actual de este, en el registro de comandos, se mostrará como *Listo*.

   Puede hacer clic en el botón **Reenviar** para enviar nuevamente el comando al dispositivo móvil del usuario.

   Puede hacer clic en el botón **Eliminar de la cola** para cancelar la ejecución de un comando enviado si este aún no se ha ejecutado.

   La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo móvil, con los respectivos estados de ejecución. Haga clic en **Actualizar** para actualizar la lista de comandos.

7. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para la administración de dispositivos móviles**.

Puede ver el perfil que ha instalado y eliminarlo, si es necesario.

## Eliminación de un perfil de configuración de un dispositivo

*Para eliminar un perfil de configuración de un dispositivo móvil:*

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En el espacio de trabajo, filtre los dispositivos MDM con iOS haciendo clic en el enlace **MDM para iOS**.

3. Seleccione el dispositivo móvil del usuario del que necesita eliminar el perfil de configuración.

   Puede seleccionar múltiples dispositivos móviles para eliminar el perfil simultáneamente.

4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

5. En la ventana **Comandos para la administración de dispositivos móviles**, vaya a la sección **Eliminar perfil** y haga clic en el botón **Enviar comando**.

   También puede enviar el comando al dispositivo móvil seleccionando **Todos los comandos** del menú contextual del dispositivo, y después seleccione **Eliminar perfil**.

   Se abre la ventana **Eliminar perfiles** que muestra una lista de perfiles.

6. Seleccione de la lista el perfil que necesita eliminar del dispositivo móvil. Puede seleccionar múltiples perfiles para eliminarlos simultáneamente del dispositivo móvil. Para seleccionar el rango de perfiles, use la tecla **Mayús**. Para combinar perfiles en un grupo, use la tecla **CTRL**.

7. Haga clic en el botón **Aceptar** para enviar el comando al dispositivo móvil.

   Cuando el comando se ejecute, el perfil de configuración seleccionado se eliminará del dispositivo móvil del usuario. Si el comando se ejecuta exitosamente, el estado actual de este se mostrará como *Completado*.

   Puede hacer clic en el botón **Reenviar** para enviar nuevamente el comando al dispositivo móvil del usuario.

   Puede hacer clic en el botón **Eliminar de la cola** para cancelar la ejecución de un comando enviado si este aún no se ha ejecutado.

   La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo móvil, con los respectivos estados de ejecución. Haga clic en **Actualizar** para actualizar la lista de comandos.

8. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para la administración de dispositivos móviles**.

## Adición de un dispositivo nuevo al publicar un enlace a un perfil

En la Consola de administración, el administrador crea un nuevo perfil de MDM para iOS, usando el Asistente de instalación de certificados. El Asistente realiza las siguientes acciones:

- El perfil de MDM para iOS se publica automáticamente en el Servidor web.
- Se envía al usuario un enlace al perfil de MDM para iOS por SMS o por correo electrónico. Para recibir el enlace, el usuario instala el perfil de MDM para iOS en el dispositivo móvil.
- El dispositivo móvil se conecta al Servidor de MDM para iOS.

Debido a una directiva de seguridad más estricta introducida por Apple, debe configurar las versiones del protocolo TLS 1.1 y TLS 1.2 al conectar un dispositivo móvil que ejecute iOS 11 a un Servidor de administración que tenga la integración con la Infraestructura de clave pública (PKI) habilitada.

## Adición de un dispositivo nuevo a través de instalación del perfil por el administrador

Para conectar un dispositivo móvil a un Servidor de MDM para iOS al instalar un perfil de MDM para iOS en ese dispositivo móvil, el administrador debe realizar las siguientes acciones:

1. En la Consola de administración, abra el Asistente de instalación de certificados.
2. Cree un nuevo perfil de MDM para iOS al seleccionar la casilla **Mostrar el certificado cuando el finalice el asistente** en la ventana del Asistente.
3. Guarda el perfil de MDM para iOS.
4. Instale el perfil de MDM para iOS en el dispositivo móvil del usuario a través de la utilidad Apple Configurator.

El dispositivo móvil se conecta al Servidor de MDM para iOS.

Debido a una directiva de seguridad más estricta introducida por Apple, debe configurar las versiones del protocolo TLS 1.1 y TLS 1.2 al conectar un dispositivo móvil que ejecute iOS 11 a un Servidor de administración que tenga la integración con la Infraestructura de clave pública (PKI) habilitada.

## Adición de un perfil de aprovisionamiento

*Para agregar un perfil de aprovisionamiento a un Servidor de MDM para iOS:*

1. En el árbol de la consola, abra la carpeta **Administración de dispositivos móviles**.
2. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Servidores de dispositivos móviles**.
3. En el espacio de trabajo de la carpeta **Servidores de dispositivos móviles**, seleccione un Servidor de MDM para iOS.
4. En el menú contextual del Servidor de MDM para iOS, seleccione **Propiedades**.

   Se abre la ventana de propiedades del servidor de dispositivos móviles.
5. En la ventana de propiedades del **Servidor de MDM para iOS**, vaya a la sección **Perfiles de aprovisionamiento**.
6. En la sección **Perfiles de aprovisionamiento**, haga clic en el botón **Importar** y especifique la ruta a un perfil de aprovisionamiento.

El perfil se agregará a la configuración del Servidor de MDM para iOS.

Puede hacer clic en el botón **Exportar** para guardar perfil de aprovisionamiento en un archivo.

Puede instalar el perfil de aprovisionamiento que ha importado en dispositivos MDM con iOS.

## Instalación de un perfil de aprovisionamiento en un dispositivo

*Para instalar un perfil de aprovisionamiento en un dispositivo móvil:*

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.
2. En el espacio de trabajo, filtre los dispositivos MDM con iOS por protocolo (*MDM para iOS*).
3. Seleccione el dispositivo móvil del usuario en el que necesita instalar el perfil de aprovisionamiento.

   Puede seleccionar múltiples dispositivos móviles para instalar el perfil de aprovisionamiento simultáneamente.
4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

5. En la ventana **Comandos para la administración de dispositivos móviles** vaya a la sección **Instalar perfil de aprovisionamiento** y haga clic en el botón **Enviar comando**.

   También puede enviar el comando al dispositivo móvil seleccionando **Todos los comandos** del menú contextual del dispositivo móvil, y después seleccione **Instalar perfil de aprovisionamiento**.

   Como resultado, se abre la ventana **Seleccionar perfiles de aprovisionamiento** que muestra una lista de perfiles de aprovisionamiento. Seleccione de la lista el perfil de aprovisionamiento que necesita instalar en el dispositivo móvil. Puede seleccionar múltiples perfiles de aprovisionamiento para instalarlos simultáneamente en el dispositivo móvil. Para seleccionar el rango de perfiles de aprovisionamiento, use la tecla **Mayús**. Para combinar perfiles de aprovisionamiento en un grupo, use la tecla **Ctrl**.

6. Haga clic en el botón **Aceptar** para enviar el comando al dispositivo móvil.

   Cuando el comando se ejecute, el perfil de aprovisionamiento seleccionado se instalará en el dispositivo móvil del usuario. Si el comando se ejecuta correctamente, su estado actual en el registro de comandos se muestra como *Completado*.

   Puede hacer clic en el botón **Reenviar** para enviar nuevamente el comando al dispositivo móvil del usuario.

   Puede hacer clic en el botón **Eliminar de la cola** para cancelar la ejecución de un comando enviado si este aún no se ha ejecutado.

   La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo móvil, con los respectivos estados de ejecución. Haga clic en **Actualizar** para actualizar la lista de comandos.

7. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para la administración de dispositivos móviles**.

Puede ver el perfil que ha instalado y eliminarlo, si es necesario.

## Eliminación de un perfil de aprovisionamiento de un dispositivo

*Para eliminar un perfil de aprovisionamiento de un dispositivo móvil:*

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En el espacio de trabajo, filtre los dispositivos MDM con iOS por protocolo (*MDM para iOS*).

3. Seleccione el dispositivo móvil del usuario del que necesita eliminar el perfil de aprovisionamiento.

   Puede seleccionar múltiples dispositivos móviles para eliminar el perfil de aprovisionamiento simultáneamente.

4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

5. En la ventana **Comandos para la administración de dispositivos móviles**, vaya a la sección **Eliminar perfil de aprovisionamiento** y haga clic en el botón **Enviar comando**

   También puede enviar el comando al dispositivo móvil seleccionando **Todos los comandos** del menú contextual, después seleccione **Eliminar perfil de aprovisionamiento**.

   Se abre la ventana **Eliminar perfiles de aprovisionamiento** que muestra una lista de perfiles.

6. Seleccione de la lista el perfil de aprovisionamiento que necesita eliminar del dispositivo móvil. Puede seleccionar múltiples perfiles de aprovisionamiento para eliminarlos simultáneamente del dispositivo móvil. Para seleccionar el rango de perfiles de aprovisionamiento, use la tecla **Mayús**. Para combinar perfiles de aprovisionamiento en un grupo, use la tecla **Ctrl**.

7. Haga clic en el botón **Aceptar** para enviar el comando al dispositivo móvil.

   Cuando el comando se ejecuta, el perfil de aprovisionamiento seleccionado se eliminará del dispositivo móvil del usuario. Las aplicaciones relacionadas con el perfil de aprovisionamiento eliminado no funcionarán. Si el comando se ejecuta exitosamente, el estado actual de este se mostrará como *Completado*.

   Puede hacer clic en el botón **Reenviar** para enviar nuevamente el comando al dispositivo móvil del usuario.

   Puede hacer clic en el botón **Eliminar de la cola** para cancelar la ejecución de un comando enviado si este aún no se ha ejecutado.

   La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo móvil, con los respectivos estados de ejecución. Haga clic en **Actualizar** para actualizar la lista de comandos.

8. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para la administración de dispositivos móviles**.

## Agregar una aplicación administrada

Antes de instalar una app en un dispositivo MDM con iOS, debe agregar esa app en un Servidor de MDM para iOS. Una aplicación se considera administrada si ha sido instalada en un dispositivo a través de Kaspersky Security Center. Una aplicación administrada puede administrarse remotamente por medio de Kaspersky Security Center.

*Para agregar una aplicación administrada a un Servidor de MDM para iOS:*

1. En el árbol de la consola, abra la carpeta **Administración de dispositivos móviles**.

2. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Servidores de dispositivos móviles**.

3. En el espacio de trabajo de la carpeta **Servidores de dispositivos móviles**, seleccione un Servidor de MDM para iOS.

4. En el menú contextual del Servidor de MDM para iOS, seleccione **Propiedades**.

   Se abre la ventana de propiedades del Servidor de MDM para iOS.

5. En la ventana de propiedades del Servidor de MDM para iOS, seleccione la sección **Aplicaciones administradas**.

6. Haga clic en el botón **Agregar** en la sección **Aplicaciones administradas**.

   Se abre la ventana **Agregar una aplicación**.

7. En la ventana **Agregar una aplicación**, en el campo **Nombre de la app**, especifique el nombre de la aplicación que desea agregar.

8. En el campo **Id. de Apple o vínculo al archivo de manifiesto** especifique la ID de Apple de la aplicación que se agregará o un enlace al archivo de manifiesto que se pueda utilizar para descargarla.

9. Si desea eliminar una aplicación administrada del dispositivo móvil del usuario junto al perfil de MDM para iOS cuando elimine este, seleccione la casilla **Eliminar junto con el perfil de MDM para iOS**.

10. Si desea bloquear la copia de seguridad de datos de la aplicación a través de iTunes, seleccione la casilla **Bloquear copia de seguridad de datos**.

11. Haga clic en **Aceptar**.

La aplicación agregada se muestra en la sección **Aplicaciones administradas** de la ventana de propiedades del Servidor de MDM para iOS.

## Instalar una app en un dispositivo móvil

*Para instalar una app en un dispositivo móvil con MDM para iOS:*

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. Seleccione el dispositivo MDM con iOS en el que desea instalar una app.

   Puede seleccionar múltiples dispositivos móviles para instalar la aplicación simultáneamente.

3. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

4. En la ventana **Comandos para la administración de dispositivos móviles**, vaya a la sección **Instalar app** y haga clic en el botón **Enviar comando**.

   También puede enviar el comando al dispositivo móvil seleccionando **Todos los comandos** del menú contextual del dispositivo móvil y después **Instalar app**.

   Se abre la ventana **Seleccionar apps** que muestra una lista de perfiles. Seleccione de la lista la aplicación que necesita instalar en el dispositivo móvil. Puede seleccionar múltiples aplicaciones para instalarlas simultáneamente en el dispositivo móvil. Para seleccionar un rango de aplicaciones, use la tecla **Mayús**. Para combinar aplicaciones en un grupo, use la tecla **Ctrl**.

5. Haga clic en el botón **Aceptar** para enviar el comando al dispositivo móvil.

   Cuando el comando se ejecute, la aplicación seleccionada se instalará en el dispositivo móvil del usuario. Si el comando se ejecuta correctamente, su estado actual en el registro de comandos se mostrará como *Completado*.

   Puede hacer clic en el botón **Reenviar** para enviar nuevamente el comando al dispositivo móvil del usuario. Puede hacer clic en el botón **Eliminar de la cola** para cancelar la ejecución de un comando enviado si este aún no se ha ejecutado.

   La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo móvil, con los respectivos estados de ejecución. Haga clic en **Actualizar** para actualizar la lista de comandos.

6. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para la administración de dispositivos móviles**.

En las propiedades del dispositivo móvil con MDM para iOS se muestra información acerca de la aplicación instalada. Puede quitar la aplicación del dispositivo móvil mediante el registro de comandos o el menú contextual del dispositivo móvil.

## Eliminar una app de un dispositivo

*Para eliminar una app de un dispositivo móvil:*

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En el espacio de trabajo, filtre los dispositivos MDM con iOS por protocolo (*MDM para iOS*).

3. Seleccione el dispositivo móvil del usuario del que necesita eliminar la app.

   Puede seleccionar múltiples dispositivos móviles para eliminar la app simultáneamente.

4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

5. En la ventana **Comandos para la administración de dispositivos móviles**, vaya a la sección **Eliminar app** y haga clic en el botón **Enviar comando**.

   También puede enviar el comando al dispositivo móvil seleccionando **Todos los comandos** del menú contextual del dispositivo móvil y después **Eliminar app**.

   Como resultado, se abre la ventana **Eliminar apps** que muestra una lista de aplicaciones.

6. Seleccione de la lista la app que necesita eliminar del dispositivo móvil. Puede seleccionar múltiples apps para eliminarlas simultáneamente. Para seleccionar un rango de aplicaciones, use la tecla **Mayús**. Para combinar aplicaciones en un grupo, use la tecla **Ctrl**.

7. Haga clic en el botón **Aceptar** para enviar el comando al dispositivo móvil.

   Cuando el comando se ejecute, la app seleccionada se eliminará del dispositivo móvil del usuario. Si el comando se ejecuta exitosamente, el estado actual de este se mostrará como *Completado*.

   Puede hacer clic en el botón **Reenviar** para enviar nuevamente el comando al dispositivo móvil del usuario.

   Puede hacer clic en el botón **Eliminar de la cola** para cancelar la ejecución de un comando enviado si este aún no se ha ejecutado.

   La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo móvil, con los respectivos estados de ejecución. Haga clic en **Actualizar** para actualizar la lista de comandos.

8. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para la administración de dispositivos móviles**.

## Configuración de roaming en un dispositivo móvil MDM con iOS

*Para configurar roaming:*

1. En el árbol de la consola, abra la carpeta **Administración de dispositivos móviles**.

2. En la carpeta **Administración de dispositivos móviles**, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

3. Seleccione el dispositivo MDM con iOS propiedad del usuario para quien debe configurar roaming.

   Puede seleccionar varios dispositivos móviles para configurar roaming en ellos simultáneamente.

4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

5. En la ventana **Comandos para la administración de dispositivos móviles**, vaya a la sección **Configurar roaming** y haga clic en el botón **Enviar comando**.

   También puede enviar el comando al dispositivo móvil al seleccionar **Todos los comandos → Configurar roaming** desde el menú contextual del dispositivo.

6. En la ventana **Configuración de roaming**, especifique los ajustes pertinentes:

   - Habilitar roaming de datos

     Si se habilita esta opción, se activa el roaming de datos en el dispositivo móvil de MDM para iOS. El usuario del dispositivo móvil de MDM para iOS puede navegar por Internet mientras está en roaming.

     Esta opción está deshabilitada de forma predeterminada.

El roaming está configurado para los dispositivos seleccionados.

## Ver la información acerca de un dispositivo MDM con iOS

*Para ver información acerca de un dispositivo MDM con iOS:*

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En el espacio de trabajo, filtre los dispositivos MDM con iOS haciendo clic en el enlace **MDM para iOS**.

3. Seleccione el dispositivo móvil sobre el que necesite información.

4. En el menú contextual del dispositivo móvil, seleccione **Propiedades**.

   Se abre la ventana de propiedades del dispositivo MDM con iOS.

La ventana de propiedades del dispositivo móvil muestra información acerca del dispositivo MDM con iOS conectado.

## Desconectar de la administración un dispositivo MDM con iOS

*Para desconectar un dispositivo MDM con iOS del Servidor de MDM para iOS:*

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En el espacio de trabajo, filtre los dispositivos MDM con iOS haciendo clic en el enlace **MDM para iOS**.

3. Seleccione el dispositivo móvil que necesita desconectar.

4. En el menú contextual del dispositivo móvil, seleccione **Eliminar**.

El dispositivo MDM con iOS se marcará en la lista para ser eliminado. El dispositivo móvil se eliminará automáticamente de la lista de dispositivos administrados después de que se elimine de la base de datos del Servidor de MDM para iOS. El dispositivo móvil se eliminará de la base de datos del Servidor de MDM para iOS en menos de un minuto.

Después de que el dispositivo MDM con iOS se desconecte de la administración, todos los perfiles de configuración instalados, el perfil de MDM para iOS, y las aplicaciones para las que se ha habilitado la opción **Eliminar junto con el perfil de MDM para iOS**, se eliminarán del dispositivo móvil.

### Envío de comandos a un dispositivo

*Para enviar un comando a un dispositivo MDM con iOS:*

1. En la Consola de administración, abra el nodo **Administración de dispositivos móviles**.
2. Seleccione la carpeta **Dispositivos móviles**.
3. En la carpeta **Dispositivos móviles**, seleccione el dispositivo móvil al cual los comandos se tienen que enviar.
4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.
5. En la lista que aparece, seleccione el comando que se debe enviar al dispositivo móvil.

### Comprobación del estado de ejecución de comandos enviada

*Para comprobar el estado de ejecución de un comando que se ha enviado a un dispositivo móvil:*

1. En la Consola de administración, abra el nodo **Administración de dispositivos móviles**.
2. Seleccione la carpeta **Dispositivos móviles**.
3. En la carpeta **Dispositivos móviles**, seleccione el dispositivo móvil en el cual el estado de ejecución se tiene que examinar para ver los comandos seleccionados.
4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

## Administración de dispositivos KES

En Kaspersky Security Center, puede administrar dispositivos móviles KES de las siguientes maneras:

- Administre centralmente los dispositivos KES mediante comandos.
- Vea información acerca de la configuración de administración de dispositivos KES.
- Instalar las aplicaciones con paquetes de apps móviles.
- Desconecte dispositivos KES de la administración.

## Crear un paquete de aplicaciones móviles para dispositivos KES

Para crear un paquete de aplicaciones móviles para dispositivos KES se requiere una licencia de Kaspersky Endpoint Security para Android.

*Para crear un paquete de aplicaciones móviles:*

1. En la carpeta **Instalación remota** del árbol de la consola, seleccione la subcarpeta **Paquetes de instalación**.

   De manera predeterminada, la carpeta **Instalación remota** es una subcarpeta de la carpeta **Avanzado**.

2. Haga clic en el botón **Acciones adicionales** y seleccione **Administrar paquetes de aplicaciones móviles** en la lista desplegable.

3. En la ventana **Administración de paquetes de aplicaciones móviles**, haga clic en el botón **Nuevo**.

4. Se inicia el Asistente de nuevo paquete. Siga las instrucciones del asistente.

El paquete de aplicaciones móviles recientemente creado se muestra en la ventana **Administración de paquetes de aplicaciones móviles**.

## Habilitar la autenticación basada en certificados para dispositivos KES

*Para habilitar la autenticación basada en certificados de un dispositivo KES:*

1. Abra el Registro del dispositivo cliente en el que está instalado el Servidor de administración (por ejemplo, de forma local con el comando regedit en el menú **Iniciar** → **Ejecutar**).

2. Vaya al siguiente archivo:

   - Para sistemas de 32 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

   - Para sistemas de 64 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

3. Cree una clave de nombre LP_MobileMustUseTwoWayAuthOnPort13292.

4. Especifique REG_DWORD como tipo de clave.

5. Asigne el valor 1 a la clave.

6. Reinicie el servicio del Servidor de administración.

Una vez que se ejecute el servicio del Servidor de administración, el uso obligatorio de la autenticación basada en certificados quedará habilitada para el dispositivo KES.

No se exigirá un certificado cuando el dispositivo KES se conecte al Servidor de administración por primera vez.

De manera predeterminada, la autenticación basada en certificados de los dispositivos KES está deshabilitada.

## Ver la información acerca de un dispositivo KES

*Para ver información acerca de un dispositivo KES:*

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En el espacio de trabajo, filtre los dispositivos KES por protocolo *(KES)*.

3. Seleccione el dispositivo móvil sobre el que necesite información.

4. En el menú contextual del dispositivo móvil, seleccione **Propiedades**.

Se abre la ventana de propiedades del dispositivo KES.

La ventana de propiedades del dispositivo móvil muestra información acerca del dispositivo KES conectado.

## Desconectar de la administración un dispositivo KES

Para desconectar de la administración un dispositivo KES, el usuario tiene que eliminar del dispositivo móvil el Agente de red. Una vez que el usuario haya eliminado el Agente de red, la información del dispositivo móvil se elimina de la base de datos del Servidor de administración, de modo que el administrador pueda eliminarlo de la lista de dispositivos administrados.

*Para eliminar un dispositivo KES de la lista de dispositivos administrados:*

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En el espacio de trabajo, filtre los dispositivos KES por protocolo *(KES)*.

3. Seleccione el dispositivo móvil que debe desconectar de la administración.

4. En el menú contextual del dispositivo móvil, seleccione **Eliminar**.

El dispositivo móvil se elimina de la lista de dispositivos administrados.

Si Kaspersky Endpoint Security para Android no se ha eliminado del dispositivo móvil, este reaparecerá en la lista de dispositivos administrados después de la sincronización con el Servidor de administración.

# Protección y cifrado de datos

El cifrado de datos reduce el riesgo de pérdida involuntaria de datos en caso de que le roben o pierda su computadora portátil, su unidad extraíble o su disco duro, o en caso de que usuarios no autorizados y aplicaciones accedan a ellos.

Kaspersky Endpoint Security para Windows proporciona funcionalidad de cifrado. Kaspersky Endpoint Security para Windows le permite cifrar archivos almacenados en unidades locales de dispositivos y unidades extraíbles, así como cifrar unidades extraíbles y unidades de disco duro en su totalidad.

Las reglas de cifrado se configuran mediante directivas en Kaspersky Security Center. Al aplicar una directiva, se realiza el cifrado y el descifrado de acuerdo con las reglas existentes.

La disponibilidad de la característica para controlar el cifrado está determinada por la configuración de la interfaz de usuario.

El administrador puede realizar las siguientes acciones:

- Configurar y realizar el cifrado o descifrado de archivos en los discos locales del dispositivo.
- Configurar y cifrar los archivos en unidades extraíbles.
- Crear reglas de acceso de la aplicación a archivos cifrados.
- Crear y entregar al usuario un archivo de clave para acceder a archivos cifrados si el cifrado de archivos está restringido en el dispositivo del usuario.
- Configurar y realizar el cifrado de la unidad de disco duro.
- Administrar el acceso de usuario a discos duros y unidades extraíbles cifradas (administrar cuentas de agente de autenticación, crear y entregar a los usuarios información sobre la solicitud para la restauración del nombre de la cuenta y la contraseña, así como claves de acceso para dispositivos cifrados).
- Ver estados de cifrado e informes sobre el cifrado de archivos.

Estas operaciones se realizan mediante el uso de herramientas integradas a Kaspersky Endpoint Security para Windows. Si desea obtener instrucciones detalladas sobre cómo realizar estas operaciones, así como una descripción de las funciones de cifrado, consulte la Ayuda en línea de Kaspersky Endpoint Security para Windows

https://support.kaspersky.com/KESWin/12.6/es-MX/127971.htm
.
Kaspersky Security Center admite la funcionalidad de administración del cifrado para dispositivos que ejecutan sistemas operativos macOS. El cifrado se configura usando herramientas de Kaspersky Endpoint Security para Mac para versiones de aplicación que admitan la funcionalidad de cifrado. Si desea obtener instrucciones detalladas sobre cómo realizar cifrados, así como una descripción de las funciones, consulte la *Guía del administrador de Kaspersky Endpoint Security for Mac*.

## Ver la lista de dispositivos cifrados

*Para ver la lista de dispositivos cifrados que almacenan información cifrada, realice lo siguiente:*

1. En el árbol de consola del Servidor de administración, seleccione la carpeta **Protección y cifrado de datos**.
2. Abra la lista de dispositivos cifrados mediante uno de los siguientes métodos:
   - Al hacer clic en el enlace **Ir a la lista de unidades cifradas** en la sección **Administrar unidades cifradas**.
   - Seleccionando la carpeta **Unidades cifradas** en el árbol de consola.

El espacio de trabajo mostrará información acerca de los dispositivos de la red que almacenan archivos cifrados y acerca de los dispositivos cifrados a nivel de unidad. Después de descifrar la información de un dispositivo, este dispositivo se elimina automáticamente de la lista.

Puede ordenar la información de la lista de dispositivos tanto en orden ascendente como descendente, en cualquier columna.

La configuración de la interfaz de usuario determina si la carpeta **Protección y cifrado de datos** aparece o no en el árbol de consola.

## Ver la lista de eventos de cifrado

Al ejecutar tareas de cifrado y descifrado de datos en los dispositivos cliente, Kaspersky Endpoint Security para Windows envía a Kaspersky Security Center información sobre los siguientes tipos de eventos:

- No se puede cifrar o descifrar un archivo, o no se puede crear un archivo de almacenamiento cifrado por falta de espacio en disco.
- No se puede cifrar o descifrar un archivo, o no se puede crear un archivo de almacenamiento cifrado debido a problemas de licencia.
- No se puede cifrar o descifrar un archivo, o no se puede crear un archivo de almacenamiento cifrado porque no se tienen los derechos de acceso necesarios.
- Se prohibió el acceso de la aplicación a un archivo cifrado.
- Errores desconocidos.

*Para ver una lista de los eventos que tuvieron lugar durante el cifrado de datos en dispositivos, realice lo siguiente:*

1. En el árbol de consola del Servidor de administración, seleccione la carpeta **Protección y cifrado de datos**.
2. Abra la lista de eventos que tuvieron lugar durante el cifrado de datos, mediante uno de los siguientes métodos:
   - Haga clic en el vínculo **Ir a la lista de errores** de la sección **Errores de cifrado de datos**.
   - Seleccione la carpeta **Unidades cifradas** en el árbol de consola.

El espacio de trabajo mostrará información acerca de los problemas que se produjeron durante el cifrado de datos en dispositivos.

Puede realizar las siguientes acciones en la lista de eventos de cifrado:

- Ordenar los registros de datos en orden ascendente o descendente, en cualquier columna.
- Realizar la búsqueda rápida de registros (por coincidencia de texto con una subcadena en cualquiera de los campos de la lista).
- Exportar la lista de eventos a un archivo de texto.

La configuración de la interfaz de usuario determina si la carpeta **Protección y cifrado de datos** aparece o no en el árbol de consola.

## Exportar la lista de eventos de cifrado en un archivo de texto

*Para exportar la lista de eventos de cifrado a un archivo de texto:*

1. Cree una lista de eventos de cifrado.
2. En el menú contextual de la lista de eventos, seleccione **Exportar lista**.

   Se abre la ventana **Exportar lista**.
3. En la ventana **Exportar lista**, especifique el nombre del archivo de texto con la lista de eventos, seleccione una carpeta para guardarlo y haga clic en el botón **Guardar**.

   La lista de eventos de cifrado se guardará en el archivo especificado.

## Crear y ver informes de cifrado

Puede generar los siguientes informes:

- Informe sobre el estado de cifrado de los dispositivos administrados. Este informe proporciona detalles sobre el cifrado de datos de varios dispositivos administrados. Por ejemplo, el informe muestra el número de dispositivos a los que se aplica la directiva con reglas de cifrado configuradas. Además, puede averiguar, entre otras cosas, cuántos dispositivos deben reiniciarse. El informe también contiene información sobre la tecnología de cifrado y el algoritmo usados en cada dispositivo.
- Informe sobre el estado de cifrado de los dispositivos de almacenamiento masivo. Este informe contiene la misma información que el informe sobre el estado de cifrado de los dispositivos administrados, pero proporciona datos solo para dispositivos de almacenamiento masivo y unidades extraíbles.
- Informe sobre derechos de acceso a unidades cifradas. Este informe muestra qué cuentas de usuario tienen acceso a unidades cifradas.

- Informe sobre los errores de cifrado de archivos. Este informe contiene información sobre errores que ocurrieron durante tareas de cifrado o descifrado de datos en dispositivos.

- Informe sobre el bloqueo de acceso a los archivos cifrados. Este informe contiene información sobre el bloqueo de acceso de las aplicaciones a los archivos cifrados. Este informe es útil si un usuario o una aplicación no autorizados intenta obtener acceso a archivos o unidades cifradas.

*Para generar el informe de cifrado de dispositivos:*

1. En el árbol de consola del Servidor de administración, seleccione la carpeta **Protección y cifrado de datos**.

2. Realice una de las siguientes acciones:

   - Para generar el informe sobre el estado de cifrado de los dispositivos administrados, haga clic en el enlace **Ver informe sobre el estado de cifrado de los dispositivos de almacenamiento masivo**.

     Si aún no ha configurado este informe, se iniciará el Asistente de nueva plantilla de informe. Siga los pasos del asistente.

   - Para generar el informe sobre el estado de cifrado de los dispositivos de almacenamiento masivo, en el árbol de la consola, seleccione la subcarpeta **Unidades cifradas** y luego haga clic en el botón **Ver informe sobre el estado de cifrado de los dispositivos de almacenamiento masivo**.

   Se inicia la generación del informe. El informe aparece en la pestaña **Informes** en el nodo del **Servidor de administración**.

*Para generar el informe sobre derechos de acceso a los dispositivos cifrados, realice lo siguiente:*

1. En el árbol de consola del Servidor de administración, seleccione la carpeta **Protección y cifrado de datos**.

2. Realice una de las siguientes acciones:

   - Haga clic en el vínculo **Informe sobre derechos de acceso a unidades cifradas** en la sección **Administrar unidades cifradas** para iniciar el Asistente de nueva plantilla de informe.

   - Seleccione la subcarpeta **Unidades cifradas**, luego haga clic en **Informe sobre derechos de acceso a unidades cifradas** para iniciar el Asistente de nueva plantilla de informe.

3. Siga los pasos del Asistente de nueva plantilla de informe.

   Se inicia la generación del informe. El informe aparece en la pestaña **Informes** en el nodo del **Servidor de administración**.

*Para generar el informe sobre los errores de cifrado de archivos:*

1. En el árbol de consola del Servidor de administración, seleccione la carpeta **Protección y cifrado de datos**.

2. Realice una de las siguientes acciones:

   - Haga clic en el vínculo **Ver informe sobre los errores de cifrado de archivos** en la sección **Errores de cifrado de archivos** para iniciar el Asistente de nueva plantilla de informe.

   - Seleccione la subcarpeta **Eventos de cifrado** y luego haga clic en el vínculo **Informe sobre los errores de cifrado de archivos** para iniciar el Asistente de nueva plantilla de informe.

3. Siga los pasos del Asistente de nueva plantilla de informe.

Se inicia la generación del informe. El informe aparece en la pestaña **Informes** en el nodo del **Servidor de administración**.

*Para generar el informe sobre el estado de cifrado de los dispositivos administrados:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la pestaña **Informes**.
3. Haga clic en el botón **Nueva plantilla de informe** para iniciar el Asistente de nueva plantilla de informe.
4. Siga las instrucciones del Asistente de nueva plantilla de informe. En la ventana **Selección del tipo de plantilla de informe**, en la sección **Otro** seleccione **Informar sobre el estado de cifrado de los dispositivos administrados**.

   Cuando finaliza el Asistente de nueva plantilla de informe, aparece una nueva plantilla de informe en el nodo del Servidor de administración, en la pestaña **Informes**.
5. En el nodo del Servidor de administración relevante en la pestaña **Informes**, seleccione la plantilla del informe que se creó durante los pasos anteriores de las instrucciones.

Se inicia la generación del informe. El informe aparece en la pestaña **Informes** en el nodo del **Servidor de administración**.

También puede visualizar los paneles de información en la pestaña **Estadísticas** del nodo del Servidor de administración para obtener información que indique si los estados de cifrado de los dispositivos y de las unidades extraíbles cumplen con la directiva de cifrado.

*Para generar el Informe sobre el bloqueo de acceso a los archivos cifrados:*

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la pestaña **Informes**.
3. Haga clic en el botón **Nueva plantilla de informe** para iniciar el Asistente de nueva plantilla de informe.
4. Siga las instrucciones del Asistente de nueva plantilla de informe. En la ventana **Selección del tipo de plantilla de informe**, en la sección **Otro**, seleccione **Informe sobre el bloqueo de acceso a los archivos cifrados**.

   Cuando finaliza el Asistente de nueva plantilla de informe, aparece una nueva plantilla de informe en el nodo del **Servidor de administración**, en la pestaña **Informes**.
5. En el nodo del **Servidor de administración** en la pestaña **Informes**, seleccione la plantilla del informe que se creó durante los pasos anteriores de las instrucciones.

Se inicia la generación del informe. El informe aparece en la pestaña **Informes** en el nodo del **Servidor de administración**.

## Transmisión de claves de cifrado entre Servidores de administración

Si se activa la función de cifrado de datos en un dispositivo administrado, la clave de cifrado se almacena en el Servidor de administración. La clave de cifrado se utiliza para acceder a los datos cifrados y para administrar la directiva de cifrado.

La clave de cifrado debe transmitirse a otro Servidor de administración en los siguientes casos:

- Cuando reconfigura el Agente de red en un dispositivo administrado para asignar el dispositivo a otro Servidor de administración. Si este dispositivo contiene datos cifrados, la clave de cifrado debe transmitirse al Servidor de administración de destino. Si no lo hace, no se pueden descifrar los datos.

- Cuando cifra una unidad extraíble conectada a un dispositivo D1 administrado por el Servidor de administración S1 y luego se conecta esta unidad extraíble a un dispositivo D2 administrado por el Servidor de administración S2. Para acceder a los datos en la unidad extraíble, la clave de cifrado debe transmitirse desde el Servidor de administración S1 al Servidor de administración S2.

- Cuando cifra un archivo en un dispositivo D1 administrado por el Servidor de administración S1 y luego intenta acceder al archivo en un dispositivo D2 administrado por el Servidor de administración S2. Para acceder al archivo, la clave de cifrado debe transmitirse desde el Servidor de administración S1 al Servidor de administración S2.

Puede transmitir claves de cifrado de las siguientes maneras:

- Automáticamente, al habilitar la opción **Usar la jerarquía de Servidores de administración para obtener las claves de cifrado** en las propiedades de dos Servidores de administración entre los cuales se debe transmitir una clave de cifrado. Si esta opción está deshabilitada para uno de los Servidores de administración, la transmisión automática de claves de cifrado no es posible.

  Cuando habilita la opción **Usar la jerarquía de Servidores de administración para obtener las claves de cifrado** en las propiedades de un Servidor de administración, el Servidor de administración envía todas las claves de cifrado almacenadas en su repositorio al Servidor de administración principal (si hubiera) un nivel hacia arriba en la jerarquía.

  Cuando trata de acceder a los datos cifrados, el Servidor de administración primero busca la clave de cifrado en su propio repositorio. Si se habilita la opción **Usar la jerarquía de Servidores de administración para obtener las claves de cifrado** y no se encuentra la clave de cifrado necesaria en el repositorio, el Servidor de administración también envía una solicitud a los Servidores de administración principales (si hubiera) para proporcionar la clave de cifrado necesaria. La solicitud se enviará a todos los Servidores de administración principales hasta el servidor que se encuentre en el nivel más alto de la jerarquía.

La opción **Usar la jerarquía de Servidores de administración para obtener las claves de cifrado** no está disponible actualmente en la interfaz de Web Console. Si no tiene acceso a la Consola de administración basada en MMC, use el Servidor de administración principal para administrar los dispositivos cifrados.

- De forma manual, exportando el archivo que contiene las claves de cifrado de un Servidor de administración e importándolas a otro.

  La exportación e importación de claves de cifrado son acciones que se incluyen en la función de Administración de claves de cifrado. Para realizar estas acciones, configure los derechos de acceso a la función para usuarios de Kaspersky Security Center de la siguiente manera:

  - Otorgue el derecho de acceso **Lectura** a la función de administración de claves de cifrado para un usuario que exporte claves de cifrado desde el Servidor de administración secundario.

  - Otorgue el derecho de acceso **Escribir** a la función de administración de claves de cifrado para un usuario que importe claves de cifrado al Servidor de administración de destino.

*Para habilitar la transmisión automática de las claves de cifrado entre los Servidores de administración dentro de la jerarquía, realice lo siguiente:*

1. En el árbol de la consola, seleccione el Servidor de administración para el que desea habilitar la transmisión automática de las claves de cifrado.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
3. En la ventana de propiedades, seleccione la sección **Algoritmo de cifrado**.
4. Habilite la opción **Usar la jerarquía de Servidores de administración para obtener las claves de cifrado**.
5. Haga clic en **Aceptar** para aplicar los cambios.

Las claves de cifrado se transmitirán a los Servidores de administración principales (si hubiera) en la próxima sincronización (el latido). Este Servidor de administración también proporcionará mediante solicitud una clave de cifrado desde su repositorio a un Servidor de administración secundario.

*Para transmitir claves de cifrado entre Servidores de administración de forma manual:*

1. En el árbol de la consola del Servidor de administración, seleccione el Servidor de administración secundario desde el cual desea transmitir claves de cifrado.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
3. En la ventana de propiedades, seleccione la sección **Algoritmo de cifrado**.
4. Haga clic en **Exportar claves de cifrado del Servidor de administración**.

   Asegúrese de que un usuario que exporte claves de cifrado desde el Servidor reciba el derecho de acceso **Lectura** a la función de administración de claves de cifrado.
5. En la ventana **Exportar claves de cifrado**:
   - Haga clic en el botón **Examinar** y, a continuación, especifique dónde desea guardar el archivo.
   - Indique la contraseña para proteger el archivo de accesos no autorizados.

     Recuerde la contraseña. Si pierde la contraseña, no podrá recuperarla. Si la pierde, debe repetir el procedimiento de exportación. Por lo tanto, escriba la contraseña en un papel y téngalo a mano.
6. Transmita el archivo a otro Servidor de administración, por ejemplo, mediante una carpeta compartida o una unidad extraíble.
7. En el Servidor de administración de destino, asegúrese de que se esté ejecutando la Consola de administración de Kaspersky Security Center.
8. En el árbol de la consola del Servidor de administración, seleccione el Servidor de administración de destino donde desea transmitir claves de cifrado.
9. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
10. En la ventana de propiedades, seleccione la sección **Algoritmo de cifrado**.

11. Haga clic en **Importar claves de cifrado al Servidor de administración**.

    Asegúrese de que un usuario que importe claves de cifrado desde el Servidor reciba el derecho de acceso **Escribir** a la función de administración de claves de cifrado.

12. En la ventana **Importar claves de cifrado**:

    - Haga clic en el botón **Examinar** y, a continuación, seleccione el archivo que contiene las claves de cifrado.
    - Escriba la contraseña.

13. Haga clic en **Aceptar**.

Las claves de cifrado se transmiten al Servidor de administración de destino.

# Repositorios de datos

Esta sección proporciona información sobre los datos almacenados en el Servidor de administración que se usan para hacer un seguimiento del estado de los dispositivos cliente y para darles mantenimiento.

La carpeta **Repositorios** del árbol de la consola muestra los datos usados para seguir los estados de los dispositivos cliente.

La carpeta **Repositorios** contiene los siguientes objetos:

- Actualizaciones descargadas por el Servidor de administración que se distribuyen a los dispositivos cliente.
- Lista de los equipos detectados en la red.
- Las claves de licencia detectadas en dispositivos cliente.
- Archivos que las aplicaciones de seguridad colocaron en carpetas de Cuarentena en dispositivos.
- Archivos colocados en Copia de seguridad en dispositivos cliente.
- Archivos pospuestos para su posterior análisis por aplicaciones de seguridad.

## Exportar una lista de objetos de repositorio a un archivo de texto

Puede exportar la lista de objetos del repositorio a un archivo de texto.

*Para exportar la lista de objetos del repositorio a un archivo de texto:*

1. En el árbol de consola, en la carpeta **Repositorios**, seleccione la subcarpeta del repositorio relevante.
2. En la subcarpeta del repositorio, seleccione **Exportar lista** en el menú contextual.

   Esto abre la ventana **Exportar lista**, en la que se puede especificar el nombre de archivo de texto y la ruta de la carpeta en la que se colocó.

# Paquetes de instalación

Kaspersky Security Center coloca paquetes de instalación de aplicaciones por Kaspersky y otros proveedores en repositorios de datos.

Un *paquete de instalación* es un conjunto de archivos requeridos para instalar una aplicación. Un paquete de instalación contiene la configuración de instalación y la configuración inicial de la aplicación que se está instalando.

Si desea instalar una aplicación en un dispositivo cliente, cree un paquete de instalación para esta aplicación o use un paquete existente. La lista de los paquetes de instalación disponibles se almacena en la carpeta **Instalación remota** del árbol de consola, en la subcarpeta **Paquetes de instalación**.

# Principales estados de los archivos en el repositorio

Las aplicaciones de seguridad analizan los archivos en los dispositivos en busca de virus conocidos y otros programas que pueden representar una amenaza, asignan estados a los archivos y colocan algunos de ellos en el repositorio.

Por ejemplo, las aplicaciones de seguridad pueden hacer lo siguiente:

- Guardar una copia de un archivo en el repositorio antes de eliminarlo
- Aislar archivos probablemente infectados en el repositorio

Los estados principales de los archivos se presentan en la tabla a continuación. En los sistemas de ayuda de los programas de seguridad puede obtener información más detallada sobre las acciones que se pueden realizar con los archivos.

Estados de archivos en el repositorio

| Nombre del estado | Descripción del estado |
|---|---|
| Infectado | El archivo tiene una sección de código de un virus conocido u otro malware cuya información se encuentra en bases de datos antivirus de Kaspersky. |
| No infectado | No se detectó ningún virus conocido ni otro malware en el archivo. |
| Advertencia | El archivo contiene un fragmento de código que coincide parcialmente con una parte de código de una amenaza conocida. |
| Probablemente infectado | El archivo contiene código modificado de un virus conocido o código que se parece a un virus que aún no es conocido para Kaspersky. |
| Colocado en carpeta por el usuario | El usuario colocó manualmente el archivo en el repositorio porque el comportamiento del archivo dio lugar a sospechas de que contiene algunas amenazas. El usuario puede analizar el archivo en busca de amenazas mediante el uso de bases de datos actualizadas. |
| Falso positivo | Una aplicación de Kaspersky asignó el estado Infectado a un archivo no infectado porque su código es similar al de un virus. Tras analizarlo nuevamente utilizando bases de datos actualizadas, el archivo se identifica como no infectado. |
| Desinfectado | El archivo se desinfectó correctamente. |
| Eliminado | El archivo fue eliminado durante el procesamiento. |
| Protegido con contraseña | El archivo no se puede procesar porque está protegido por contraseña. |

# Activación de reglas en modo Aprendizaje inteligente

Esta sección proporciona información sobre las detecciones realizadas en los dispositivos cliente por las reglas del Control de anomalías adaptativo de Kaspersky Endpoint Security para Windows.

Las reglas detectan y pueden bloquear comportamientos anómalos en los dispositivos cliente. Si las reglas funcionan en el modo Aprendizaje inteligente, detectan un comportamiento anómalo y envían informes sobre cada incidente al Servidor de administración de Kaspersky Security Center. La información transmitida se almacena en forma de lista en la subcarpeta **Activación de reglas en el estado Aprendizaje inteligente** de la carpeta **Repositorios**. Puede confirmar si las detecciones son válidas o agregarlas como exclusiones para que el tipo de comportamiento deje de considerarse anómalo.

La información sobre las detecciones se almacena en el registro de eventos del Servidor de administración (junto con otros eventos) y en el informe del Control de anomalías adaptativo.

Para obtener más información acerca del Control de anomalías adaptativo, las reglas, sus modos y sus estados, consulte la Ayuda de Kaspersky Endpoint Security para Windows

https://support.kaspersky.com/KESWin/12.6/es-MX/176744.htm
.

## Cómo ver la lista de detecciones realizadas con las reglas del Control de anomalías adaptativo

*Para ver la lista de detecciones realizadas por las reglas del Control de anomalías adaptativo:*

1. En el árbol de la consola, seleccione el nodo del Servidor de administración con el que desee trabajar.
2. Selecciona la subcarpeta **Activación de reglas en el estado Aprendizaje inteligente** (por defecto, esta es una subcarpeta de **Avanzado** → **Repositorios**).

   La lista muestra la siguiente información sobre las detecciones realizadas con las reglas del Control de anomalías adaptativo:

   - **Grupo de administración**

     El nombre del grupo de administración al que pertenece el dispositivo.

   - **Nombre del dispositivo**

     El nombre del dispositivo cliente en el que se aplicó la regla.

   - **Nombre**

     El nombre de la regla que se aplicó.

   - **Estado**

     **Excluyendo**. Este estado indica que el administrador procesó el elemento y lo agregó como exclusión a las reglas. El estado se mantiene hasta la siguiente sincronización del dispositivo cliente con el Servidor de administración; después de la sincronización, el elemento desaparece de la lista.

     **Confirmando**. Este estado indica que el administrador procesó y confirmó el elemento. El estado se mantiene hasta la siguiente sincronización del dispositivo cliente con el Servidor de administración; después de la sincronización, el elemento desaparece de la lista.

     Si no se muestra ningún valor, el administrador no ha procesado el elemento.

   - **Número total de veces que fueron activadas las reglas**

     El número de detecciones correspondientes a una regla heurística, un proceso y un dispositivo cliente. Kaspersky Endpoint Security cuenta este número.

   - **Nombre de usuario**

     El nombre del usuario del dispositivo cliente que ejecutó el proceso que generó la detección.

   - **Ruta del proceso de origen**

Ruta al proceso de origen, es decir, al proceso que realiza la acción (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Hash del proceso de origen**

  Hash SHA256 del archivo del proceso de origen (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Ruta del objeto de origen**

  Ruta al objeto que inició el proceso (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Hash del objeto de origen**

  Hash SHA256 del archivo de origen (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Ruta del proceso de destino**

  Ruta al proceso de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Hash del proceso de destino**

  Hash SHA256 del archivo de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Ruta del objeto de destino**

  Ruta al objeto de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Hash del objeto de destino**

  Hash SHA256 del archivo de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Procesado**

  Fecha en la que se detectó la anomalía.

*Para ver las propiedades de cada elemento de información:*

1. En el árbol de la consola, seleccione el nodo del Servidor de administración con el que desee trabajar.
2. Selecciona la subcarpeta **Activación de reglas en el estado Aprendizaje inteligente** (por defecto, esta es una subcarpeta de **Avanzado** → **Repositorios**).
3. En el espacio de trabajo **Activación de reglas en el estado Aprendizaje inteligente**, seleccione el objeto que desee.
4. Realice una de las siguientes acciones:

   - Haga clic en el enlace **Propiedades** en el cuadro de información que aparece en el lado derecho de la pantalla.
   - Haga clic derecho y, en el menú contextual, seleccione **Propiedades**.

   Se abre la ventana de propiedades del objeto, que muestra información sobre el elemento seleccionado.

Puede confirmar o excluir cualquier elemento que aparezca en la lista de detecciones de las reglas del Control de anomalías adaptativo.

*Para confirmar un elemento:*

Seleccione un elemento (o varios elementos) en la lista de detecciones y haga clic en el botón **Confirmar**.

El estado del elemento (o de los elementos) cambiará a **Confirmando**.

Su confirmación contribuirá a las estadísticas utilizadas por las reglas (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security 11 para Windows).

*Para agregar un elemento como exclusión:*

Haga clic con el botón derecho en un elemento (o varios elementos) de la lista de detecciones y seleccione **Agregar a exclusiones** en el menú contextual.

Se iniciará el Asistente para agregar exclusiones. Siga las instrucciones del asistente.

Si rechaza o confirma un elemento, se lo excluirá de la lista de detecciones la siguiente vez que el dispositivo cliente se sincronice con el Servidor de administración. El elemento dejará de aparecer en la lista.

## Adición de exclusiones para las reglas del Control de anomalías adaptativo

El Asistente para agregar exclusiones le permite agregar exclusiones a las reglas de Control de anomalías adaptativo para Kaspersky Endpoint Security.

Puede iniciar el Asistente usando alguno de los tres métodos que se describen a continuación.

*Para iniciar el Asistente para agregar exclusiones a través del nodo Control de anomalías adaptativo:*

1. En el árbol de la consola, seleccione el nodo del Servidor de administración requerido.
2. Seleccione **Activación de reglas en el estado Aprendizaje inteligente** (por defecto, esta es una subcarpeta de **Avanzado → Repositorios**).
3. En el espacio de trabajo, haga clic con el botón derecho en un elemento (o varios elementos) de la lista de detecciones y seleccione **Agregar a exclusiones** en el menú contextual.

   Puede agregar hasta 1000 exclusiones a la vez. Si selecciona más elementos e intenta agregarlos a las exclusiones, verá un mensaje de error.

Se iniciará el Asistente para agregar exclusiones.

Puede iniciar el Asistente para agregar exclusiones desde otros nodos del árbol de la consola:

- La pestaña **Eventos** de la ventana principal del Servidor de administración (y, luego, la opción **Solicitudes de usuario** o la opción **Eventos recientes**).
- El **Informe sobre el estado de las reglas del Control de anomalías adaptativo**, columna **Número de detecciones**.

### Paso 1. Seleccionar la aplicación

Este paso se puede omitir si solo tiene una versión de Kaspersky Endpoint Security para Windows y no tiene otras aplicaciones compatibles con las reglas del Control de anomalías adaptativo.

El Asistente para agregar exclusiones muestra la lista de aplicaciones de Kaspersky cuyos complementos de administración le permiten agregar exclusiones a las directivas para estas aplicaciones. Seleccione una aplicación de esta lista y haga clic en **Siguiente** para proceder a seleccionar la directiva a la que se añadirá la exclusión.

### Paso 2. La selección de la directiva (directivas)

El Asistente muestra la lista de directivas (con perfiles de directivas) para Kaspersky Endpoint Security.

Seleccione todas las directivas y perfiles a los cuales desea agregar exclusiones y haga clic en **Siguiente**.

### Paso 3. Procesamiento de la directiva (directivas)

El Asistente muestra una barra de progreso mientras se procesan las directivas. Puede hacer clic en **Cancelar** para interrumpir el procesamiento de las directivas.

Las directivas heredadas no se pueden actualizar. Si no tiene los derechos para modificar una directiva, esa directiva tampoco se actualizará.

Cuando todas las directivas se hayan procesado (o si interrumpe el procesamiento), aparecerá un informe. El informe muestra qué directivas se actualizaron correctamente (ícono verde) y qué directivas no se actualizaron (ícono rojo).

Este es el último paso del Asistente. Haga clic en **Finalizar** para cerrar el Asistente.

## Cuarentena y Copia de seguridad

Como resultado de un análisis, las aplicaciones antivirus de Kaspersky instaladas en los dispositivos cliente pueden poner archivos en Cuarentena o en Copia de seguridad.

*Cuarentena* es un repositorio especial en el que se almacenan aquellos archivos que probablemente estén infectados con virus y aquellos que no se pueden desinfectar al momento de la detección.

*Copia de seguridad* se ha diseñado para almacenar copias de seguridad de los archivos que se eliminan o modifican durante el proceso de desinfección.

Kaspersky Security Center genera una lista resumida de archivos puestos en Cuarentena o Copia de seguridad por aplicaciones de Kaspersky en los dispositivos. El Agente de red de cada dispositivo cliente se comunica con el Servidor de administración para transmitirle información sobre los archivos en Cuarentena y Copia de seguridad. Puede usar la Consola de administración para ver las propiedades de los archivos almacenados en los repositorios de los dispositivos, analizar esos repositorios en busca de malware y eliminar los archivos almacenados. Los iconos de estado de los archivos se describen en el apéndice.

Las operaciones con Cuarentena y Copia de seguridad son compatibles con Kaspersky Endpoint Security.

Kaspersky Security Center no copia archivos desde repositorios del Servidor de administración. Los archivos quedan almacenados en los repositorios de los dispositivos. Puede restaurar un archivo solo en el dispositivo con la aplicación antivirus, que colocó ese archivo en el repositorio.

## Habilitar la administración remota para archivos en repositorios

De manera predeterminada, no es posible administrar los archivos ubicados en los repositorios de los dispositivos cliente.

*Para habilitar la administración remota de los archivos almacenados en los repositorios de los dispositivos cliente:*

1. En el árbol de consola, seleccione un grupo de administración, para el cual desee habilitar la administración remota de los archivos del repositorio.
2. En el espacio de trabajo del grupo, abra la pestaña **Directivas**.
3. En la pestaña **Directivas**, seleccione la directiva de la aplicación de seguridad que coloque los archivos en los repositorios de dispositivos.
4. En la ventana de configuraciones de directiva del grupo de configuraciones **Transferencia de datos al Servidor de administración**, seleccione las casillas correspondientes a los repositorios para los cuales desea habilitar la administración remota.

   La ubicación del grupo de configuraciones **Transferencia de datos al Servidor de administración** de la ventana de propiedades de directivas y los nombres de las casillas dependen de la aplicación de seguridad que se usa actualmente.

## Visualizar propiedades de un archivo colocado en repositorio

*Para ver las propiedades de un archivo en Cuarentena o Copia de seguridad:*

1. En el árbol de consola, seleccione la carpeta **Repositorios** y la subcarpeta **Cuarentena** o **Copia de seguridad**.
2. En el espacio de trabajo de la carpeta **Cuarentena** (**Copia de seguridad**), seleccione el archivo cuyas propiedades desea ver.
3. Al seleccionar **Propiedades** en el menú contextual del archivo.

## Eliminar archivos de los repositorios

*Para eliminar un archivo de Cuarentena o Copia de seguridad:*

1. En el árbol de la consola, en la carpeta **Repositorios**, seleccione la subcarpeta **Cuarentena** o **Copia de seguridad**.
2. En el espacio de trabajo de la carpeta **Cuarentena** (o **Copia de seguridad**), seleccione los archivos que desea eliminar con las teclas **Shift** y **Ctrl**.
3. Elimine los archivos de una de las siguientes formas:
   - Al seleccionar **Eliminar** en el menú contextual de los archivos.
   - Al hacer clic en el enlace **Eliminar** (**Eliminar**) si desea borrar un solo archivo) en el cuadro de información de los archivos seleccionados.

Las aplicaciones de seguridad que colocaron los archivos en repositorios de dispositivos cliente eliminarán los archivos en estos repositorios.

## Restaurar archivos desde los repositorios

*Para restaurar un archivo desde Cuarentena o Copia de seguridad:*

1. En el árbol de consola, seleccione la carpeta **Repositorios** y la subcarpeta **Cuarentena** o **Copia de seguridad**.
2. En el espacio de trabajo de la carpeta **Cuarentena** (**Copia de seguridad**), seleccione los archivos que desea restaurar mediante las teclas **Mayús** y **Ctrl**.
3. Comience a restaurar los archivos de una de las siguientes formas:
   - Al seleccionar **Restaurar** en el menú contextual de los archivos.
   - Haciendo clic en el enlace **Restaurar** en el cuadro de información de los archivos seleccionados.

Las aplicaciones de seguridad que colocaron los archivos en repositorios de dispositivos cliente restaurarán los archivos a sus carpetas originales.

### Guardar un archivo desde los repositorios al disco

Kaspersky Security Center le permite guardar en el disco copias de archivos que fueron colocados por una aplicación de seguridad en Cuarentena o Copia de seguridad en un dispositivo cliente. Los archivos se copian al dispositivo donde se instaló Kaspersky Security Center, a la carpeta especificada.

*Para guardar en el disco duro una copia de un archivo almacenado en Cuarentena o en Copia de seguridad:*

1. En el árbol de consola, seleccione la carpeta **Repositorios** y la subcarpeta **Cuarentena** o **Copia de seguridad**.
2. En el espacio de trabajo de la carpeta **Cuarentena** (**Copia de seguridad**), seleccione un archivo que desea copiar al disco duro.
3. Comience a copiar de una de las siguientes formas:
   - Al seleccionar **Guardar en disco** en el menú contextual del archivo.
   - Haciendo clic en el enlace **Guardar en disco** en el cuadro de información del archivo seleccionado.

La aplicación de seguridad que colocó el archivo en Cuarentena en el dispositivo cliente guardará una copia del archivo en la carpeta especificada.

### Escaneo de archivos en Cuarentena

*Para analizar archivos en cuarentena:*

1. En el árbol de la consola, seleccione la carpeta **Repositorios**, la subcarpeta **Cuarentena**.
2. En el espacio de trabajo de la carpeta **Cuarentena**, seleccione los archivos que desea analizar con las teclas **`Mayús`** y **`Ctrl`**.
3. Inicie el análisis de archivos de una de las siguientes formas:
   - Al seleccionar **Analizar** en el menú contextual del archivo.
   - Mediante un clic en el enlace **Analizar** en la casilla de información de los archivos seleccionados.

   La aplicación ejecuta la tarea de análisis a pedido para aplicaciones de seguridad que colocaron los archivos seleccionados en Cuarentena en los dispositivos donde se almacenan esos archivos.

## Amenazas activas

La información sobre los archivos no procesados que se detectaron en los dispositivos cliente se almacena en la carpeta **Repositorios**, subcarpeta **Amenazas activas**.

El procesamiento y la desinfección pospuestos los lleva a cabo la aplicación de seguridad a petición o después de tener lugar un evento especificado. Puede configurar el procesamiento aplazado.

## Desinfección de un archivo no procesado

*Para iniciar la desinfección de un archivo no procesado:*

1. En el árbol de consola, en la carpeta **Repositorios**, seleccione la subcarpeta **Amenazas activas**.
2. En el espacio de trabajo de la carpeta **Amenazas activas**, seleccione el archivo que desea desinfectar.
3. Comience la desinfección de los archivos de una de las siguientes formas:
   - Al seleccionar **Desinfectar** en el menú contextual del archivo.
   - Haciendo clic en el enlace **Desinfectar** en el cuadro de información del archivo seleccionado.

   A continuación, se ejecuta el intento de desinfectar este archivo.

Si el archivo se desinfecta, la aplicación de seguridad instalada en el dispositivo cliente lo restaura a su carpeta original. El registro sobre el archivo será eliminado de la lista en la carpeta **Amenazas activas**. Si el archivo no se puede desinfectar, la aplicación de seguridad instalada en el dispositivo lo elimina desde ese dispositivo. El registro sobre el archivo será eliminado de la lista en la carpeta **Amenazas activas**.

La capacidad de desinfección y eliminación de archivos puede variar según la aplicación de seguridad instalada, su versión y configuración.

## Guardar un archivo no procesado en disco

Kaspersky Security Center permite guardar en el disco copias de archivos no procesados detectados en dispositivos cliente. Esto se refiere a los archivos tratados o eliminados por la aplicación. Los archivos se copian al dispositivo donde está instalado Kaspersky Security Center, en la carpeta que usted especifique.

Puede guardar copias de los archivos si los archivos se eliminaron o modificaron durante la desinfección y sus copias están almacenadas en el almacenamiento de Kaspersky Endpoint Security para Windows en el dispositivo administrado.

*Para guardar una copia de archivo no procesado en el disco:*

1. En el árbol de consola, en la carpeta **Repositorios**, seleccione la subcarpeta **Amenazas activas**.
2. En el espacio de trabajo de la carpeta **Amenazas activas**, seleccione los archivos que debe copiar al disco.
3. Comience a copiar de una de las siguientes formas:
   - Al seleccionar **Guardar en disco** en el menú contextual del archivo.
   - Haciendo clic en el enlace **Guardar en disco** en el cuadro de información del archivo seleccionado.

La aplicación de seguridad instalada en el dispositivo cliente en que se detectó un archivo no procesado guarda una copia del archivo en la carpeta especificada.

### Eliminar archivos desde la carpeta "Amenazas activas"

*Para eliminar un archivo desde la carpeta **Amenazas activas**:*

1. En el árbol de consola, en la carpeta **Repositorios**, seleccione la subcarpeta **Amenazas activas**.
2. En el espacio de trabajo de la carpeta **Amenazas activas**, seleccione los archivos que debe eliminar mediante las teclas **Mayús** y **Ctrl**.
3. Elimine los archivos de una de las siguientes formas:
   - Al seleccionar **Eliminar** en el menú contextual de los archivos.
   - Al hacer clic en el enlace **Eliminar** (**Eliminar** si desea borrar un solo archivo) en el cuadro de información de los archivos seleccionados.

Como resultado, las aplicaciones de seguridad que colocaron los archivos en repositorios de dispositivos cliente eliminarán los archivos desde estos repositorios. Los registros de los archivos serán eliminados de la lista en la carpeta **Amenazas activas**.

# Kaspersky Security Network (KSN)

En esta sección se describe cómo usar la infraestructura de servicios en línea llamada Kaspersky Security Network (KSN). Aquí encontrará información detallada sobre KSN e instrucciones para habilitar KSN, configurar el acceso a KSN y ver las estadísticas de uso del servidor proxy de KSN.

Es posible que la funcionalidad de las actualizaciones (incluida la provisión de actualizaciones de firmas antivirus y actualizaciones de base de código) y la funcionalidad de KSN no estén disponibles en el software en los EE. UU.

## Acerca de KSN

Kaspersky Security Network (KSN) es una infraestructura de servicios en línea que brinda acceso a la base de conocimientos en línea de Kaspersky, que contiene información sobre la reputación de los archivos, los recursos web y el software. El uso de los datos de Kaspersky Security Network garantiza una respuesta más rápida de las aplicaciones de Kaspersky ante las amenazas, mejora la eficacia de algunos componentes de protección y reduce el riesgo de falsos positivos. KSN permite utilizar las bases de datos de reputación de Kaspersky para obtener información sobre las aplicaciones instaladas en los dispositivos administrados.

Kaspersky Security Center es compatible con las siguientes soluciones de infraestructura:

- *KSN*. Esta solución permite intercambiar información con Kaspersky Security Network. Al participar en KSN, acepta enviar a Kaspersky, de manera automática, información sobre el funcionamiento de las aplicaciones de Kaspersky instaladas en los dispositivos cliente que se administran mediante Kaspersky Security Center. La información se transfiere de conformidad con la configuración de acceso a KSN. Los analistas de Kaspersky realizan un examen adicional de la información recibida y la suman a las bases de datos de estadísticas y de reputación de Kaspersky Security Network. Kaspersky Security Center utiliza esta solución de forma predeterminada.

- *Kaspersky Private Security Network (KPSN)* es una solución que permite a los usuarios de dispositivos con aplicaciones de Kaspersky instaladas obtener acceso a bases de datos de reputación de Kaspersky Security Network y otros datos estadísticos, sin enviar datos a KSN Global desde sus propios dispositivos. KPSN diseñada para clientes corporativos que, por alguno de los siguientes motivos, no pueden participar en Kaspersky Security Network:

  - Los dispositivos de los usuarios no tienen acceso a Internet.

  - La transmisión de datos fuera del país o de la LAN corporativa está prohibida por ley o por las directivas de seguridad corporativas.

  Puede configurar los ajustes de acceso de Kaspersky Private Security Network en la sección **Configuración del proxy de KSN** de la ventana de propiedades del Servidor de administración.

La aplicación le preguntará si desea unirse a KSN cuando ejecute el Asistente de inicio rápido. Puede iniciar o detener el uso de KSN en cualquier momento cuando use la aplicación.

Utiliza KSN de acuerdo con la Declaración de KSN que lee y acepta cuando habilita KSN. Si se actualiza la Declaración de KSN, se le mostrará cuando actualice una versión del Servidor de administración. Puede aceptar la Declaración de KSN actualizada o rechazarla. Si la rechaza, seguirá usando KSN de acuerdo con la versión anterior de la Declaración de KSN que aceptó anteriormente.

Cuando KSN está habilitado, Kaspersky Security Center comprueba que haya acceso a los servidores de KSN. Si los servidores DNS configurados en el sistema no permiten acceder a los servidores de Kaspersky, la aplicación utiliza servidores DNS públicos. Esto se hace para garantizar que los dispositivos administrados no vean afectado su nivel de seguridad.

Los dispositivos cliente administrados por el Servidor de administración interactúan con KSN mediante el servidor proxy de KSN. El servidor proxy de KSN proporciona las funciones siguientes:

- Permite que los dispositivos cliente envíen solicitudes a KSN, obtengan información de KSN y transfieran información a KSN, incluso cuando no tengan acceso directo a Internet.

- El servidor proxy de KSN almacena en caché los datos procesados y reduce, de esta manera, la carga en el canal de salida y el período de tiempo que se utiliza para esperar información solicitada por un dispositivo cliente.

Puede configurar el servidor proxy de KSN en la sección **Configuración del proxy de KSN** de la ventana de propiedades del Servidor de administración.

## Configuración del acceso a Kaspersky Security Network

Puede configurar el acceso a Kaspersky Security Network (KSN) en el Servidor de administración y en un punto de distribución.

*Para configurar el acceso del Servidor de administración a Kaspersky Security Network (KSN):*

1. En el árbol de consola, seleccione el Servidor de administración para el que desea configurar el acceso a KSN.

2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.

3. En la ventana de propiedades del Servidor de administración, en el panel **Secciones** seleccione **Proxy de KSN → Configuración del proxy de KSN**.

4. En el espacio de trabajo, active la opción **Usar el Servidor de administración como servidor proxy** para usar el servicio del proxy de KSN.

   Los datos se envían desde los dispositivos cliente a KSN de acuerdo con la directiva de Kaspersky Endpoint Security activa en esos dispositivos. Si se desactiva esta casilla, no se enviarán datos a KSN desde el Servidor de administración y los dispositivos cliente a través de Kaspersky Security Center. Sin embargo, los dispositivos cliente podrán enviar datos directamente a KSN (es decir, sin pasar por Kaspersky Security Center), según lo determine su configuración. La directiva de Kaspersky Endpoint Security para Windows, que está activa en los dispositivos cliente, determina qué datos se enviarán directamente (es decir, sin pasar por Kaspersky Security Center) de los dispositivos a KSN.

5. Habilite la opción **Acepto utilizar Kaspersky Security Network**.

   Si se habilita esta opción, los dispositivos cliente enviarán los resultados de instalación de parches a Kaspersky. Al activar esta opción, asegúrese de leer y aceptar los términos de la Declaración de KSN.

   If you use Kaspersky Private Security Network, enable the **Configurar KPSN** option and haga clic en el botón **Archivo de configuración del proxy de KSN** to download the KPSN configuration (files with pkcs7 and pem extensions). Una vez descargada la configuración, la interfaz muestra el nombre y contactos del proveedor, así como la fecha de creación del archivo con la configuración de KPSN.

   > Cuando habilite KPSN, preste atención a los puntos de distribución configurados para enviar solicitudes de KSN directamente a Cloud KSN. Los puntos de distribución que tengan instalado el Agente de red versión 11 (o versiones anteriores) continuarán enviando solicitudes KSN a Cloud KSN. Para reconfigurar los puntos de distribución a fin de enviar solicitudes de KSN a KPSN, habilite la opción **Reenviar solicitudes KSN al Servidor de administración** para cada punto de distribución. Puede habilitar esta opción en las propiedades del punto de distribución o en la directiva del Agente de red.

   Cuando selecciona la casilla de verificación **Configurar KPSN**, aparece un mensaje con detalles sobre KPSN.

   Si activa la opción **Configurar KPSN** en Kaspersky Security Center, estas aplicaciones reciben información sobre el soporte de KPSN. En la ventana de configuración de la aplicación, en la subsección de **Kaspersky Security Network** de la sección **Protección avanzada contra amenazas**, se muestra la información sobre el proveedor KSN seleccionado: KSN o KPSN.

   > Si usa versiones de la aplicación anteriores a Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 o anterior a Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent al ejecutar KPSN, recomendamos que use Servidores de administración secundarios para los cuales el uso de KPSN no esté habilitado.

   > Kaspersky Security Center no envía ningún dato estadístico a Kaspersky Security Network si se configura KPSN en la sección **Proxy de KSN → Configuración del proxy de KSN** en la ventana de propiedades del Servidor de administración.

   Si tiene configuró el servidor proxy en las propiedades del Servidor de administración, pero su arquitectura de red requiere que use KPSN directamente, habilite la opción **No usar el servidor proxy configurado para conectarse a KSN**. De lo contrario, las solicitudes de las aplicaciones administradas no podrán llegar a KPSN.

6. Configure la conexión del Servidor de administración al servicio del proxy de KSN:

   - En **Configuración de conexión**, en el campo **Puerto TCP**, ingrese el número del puerto TCP que se utilizará para conectarse al servidor proxy de KSN. El puerto predeterminado para conectarse al servidor proxy de KSN es el 13111.

   - Si desea que el Servidor de administración se conecte al servidor proxy de KSN a través de un puerto UDP, habilite la opción **Usar puerto UDP** e ingrese el número de puerto en el campo **Puerto UDP**. Esta opción está desactivada de forma predeterminada y se utiliza el puerto TCP. Si habilita esta opción, de forma predeterminada, se usará el puerto UDP 15111 para establecer conexión con el servidor proxy de KSN.

   - Si desea que el Servidor de administración se conecte al servidor proxy de KSN a través de un puerto HTTPS, habilite la opción **Usar HTTPS a través de este puerto** y especifique un número de puerto. Esta opción está desactivada de forma predeterminada y se utiliza el puerto TCP. Si habilita esta opción, el puerto HTTPS predeterminado de conexión al servidor proxy de KSN es 17111.

7. Habilite la opción **Conectar los servidores de administración secundarios a KSN mediante el Servidor de administración principal**.

   Cuando esta opción está habilitada, los servidores de administración secundarios de cualquier nivel de la jerarquía utilizan el Servidor de administración principal como servidor proxy de KSN. Si esta opción está desactivada, los Servidores de administración secundarios se conectan a KSN por sus propios medios. En este caso, los dispositivos administrados usan Servidores de administración secundarios como servidores proxy de KSN.

   > Los Servidores de administración secundarios usan el Servidor de administración principal como un servidor proxy si en el panel derecho de la sección **Configuración del proxy de KSN**, en las propiedades de los Servidores de administración secundarios, la casilla de verificación **Usar el Servidor de administración como servidor proxy** está seleccionada.

8. Haga clic en **Aceptar**.

Se guardará la configuración de acceso a KSN.

También puede configurar el acceso de puntos de distribución a KSN, por ejemplo, si desea reducir la carga en el Servidor de administración. El punto de distribución que actúa como un servidor proxy KSN envía solicitudes de KSN desde dispositivos administrados a Kaspersky directamente, sin utilizar el Servidor de administración.

*Para configurar el acceso del punto de distribución a Kaspersky Security Network (KSN):*

1. Asegúrese de que el punto de distribución se asigne manualmente.
2. En el árbol de consola, haga clic el nodo del **Servidor de administración**.
3. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
4. En la ventana de propiedades del Servidor de administración, seleccione la sección **Puntos de distribución**.
5. Seleccione el punto de distribución en la lista y haga clic en el botón **Propiedades** para abrir la ventana de propiedades.
6. En la ventana de propiedades del punto de distribución, en la sección **Proxy de KSN**, seleccione **Acceder a KSN en la nube/KSN directamente a través de Internet**.
7. Haga clic en **Aceptar**.

El punto de distribución actuará como servidor proxy de KSN.

## Habilitar y deshabilitar KSN

*Para habilitar KSN:*

1. En el árbol de consola seleccione el Servidor de administración para el que necesita habilitar KSN.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
3. En la ventana de propiedades del Servidor de administración, en la sección **Proxy de KSN** seleccione la subsección **Configuración del proxy de KSN**.

4. Seleccione el **Usar el Servidor de administración como servidor proxy**.

   Se habilita el servidor proxy de KSN.

5. Marque la casilla **Acepto utilizar Kaspersky Security Network**.

   KSN se habilitará.

   Si se selecciona esta casilla, los dispositivos cliente enviarán los resultados de instalación del parche a Kaspersky. Al seleccionar esta casilla, debe leer y aceptar los términos de la Declaración de KSN.

6. Haga clic en **Aceptar**.

*Para deshabilitar KSN:*

1. En el árbol de consola seleccione el Servidor de administración para el que necesita habilitar KSN.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
3. En la ventana de propiedades del Servidor de administración, en la sección **Proxy de KSN** seleccione la subsección **Configuración del proxy de KSN**.
4. Desmarque las casillas de verificación **Utilizar el Servidor de administración como servidor proxy** o **Acepto utilizar Kaspersky Security Network** para deshabilitar el servicio del proxy de KSN.

   Si se desactiva esta casilla, los dispositivos cliente no enviarán los resultados de instalación del parche a Kaspersky.

   Si está usando KPSN, desactive la casilla de verificación **Configurar KPSN**.

   KSN se deshabilitará.

5. Haga clic en **Aceptar**.

## Ver la Declaración de KSN aceptada

Para habilitar Kaspersky Security Network (KSN), debe leer y aceptar la Declaración de KSN. Si ya ha aceptado la Declaración de KSN y quiere verla nuevamente, puede hacerlo en cualquier momento.

*Para ver la Declaración de KSN aceptada:*

1. En el árbol de consola seleccione el Servidor de administración para el que habilitó KSN.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
3. En la ventana de propiedades del Servidor de administración, en la sección **Proxy de KSN** seleccione la subsección **Configuración del proxy de KSN**.
4. Haga clic en el vínculo **Ver la Declaración de KSN aceptada**.

En la ventana que se abre, puede ver el texto de la Declaración de KSN aceptada.

## Ver las estadísticas del servidor proxy de KSN

El *servidor proxy de KSN* es un servicio que asegura la interacción entre la infraestructura de Kaspersky Security Network y los dispositivos cliente administrados por el Servidor de administración.

El uso de un servidor proxy de KSN ofrece las siguientes funciones:

- Permite que los dispositivos cliente envíen solicitudes e información a KSN incluso si no tienen acceso directo a Internet.
- El servidor proxy de KSN almacena en caché los datos procesados y reduce, de esta manera, la carga en el canal de salida y el período de tiempo que se utiliza para esperar información solicitada por un dispositivo cliente.

En la ventana de propiedades del Servidor de administración, puede configurar el servidor proxy de KSN y ver estadísticas sobre su uso.

*Para ver las estadísticas del servidor proxy de KSN:*

1. En el árbol de consola, seleccione el Servidor de administración para el que necesita ver las estadísticas de KSN.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
3. En la ventana de propiedades del Servidor de administración, en la sección **Proxy de KSN**, seleccione la subsección **Estadísticas del proxy de KSN**.

   En esta sección, se muestran las estadísticas reales del funcionamiento del servidor proxy KSN (la cantidad de registros de caché, paquetes procesados en caché y paquetes recibidos). Además, si el Servidor de administración está conectado a KSN, se mostrará el mensaje informativo correspondiente.

   De ser necesario, realice las siguientes acciones adicionales:

   - Haga clic en el botón **Actualizar** para actualizar las estadísticas sobre el uso del servidor proxy de KSN.
   - Haga clic en el botón **Exportar a archivo** para exportar las estadísticas a un archivo CSV.
   - Haga clic en el botón **Verificar conexión a KSN** para comprobar si el Servidor de administración se encuentra conectado a KSN.
4. Haga clic en el botón **Aceptar** para cerrar la ventana de propiedades del Servidor de administración.

## Aceptar una Declaración de KSN actualizada

Utiliza KSN de acuerdo con la Declaración de KSN que lee y acepta cuando habilita KSN. Si se actualiza la Declaración de KSN, se le muestra cuando actualiza el Servidor de administración. Puede aceptar la Declaración de KSN actualizada o rechazarla. Si la rechaza, seguirá usando KSN de acuerdo con la versión de la Declaración de KSN que aceptó anteriormente.

Después de actualizar o mejorar el Servidor de administración, la Declaración de KSN actualizada se muestra automáticamente. Si rechaza la Declaración de KSN actualizada, puede verla y aceptarla más adelante.

*Para ver y luego aceptar o rechazar una Declaración de KSN actualizada:*

1. En el árbol de consola, haga clic el nodo del **Servidor de administración**.
2. En la pestaña **Supervisión**, en la sección **Supervisión**, haga clic en el vínculo **La Declaración de Kaspersky Security Network aceptada es obsoleta**.

   Se abre la ventana **Declaración de KSN**.
3. Lea atentamente la Declaración de KSN y, a continuación, tome su decisión. Si acepta la Declaración de KSN actualizada, haga clic en el botón **Acepto los términos del Contrato de licencia**. Si rechaza la Declaración de KSN actualizada, haga clic en el botón **Cancelar**.

Según su elección, KSN sigue funcionando de acuerdo con los términos de la Declaración de KSN actual o actualizada. Puede ver el texto de la Declaración de KSN aceptada en las propiedades del Servidor de administración en cualquier momento.

## Mejor protección con Kaspersky Security Network

Kaspersky ofrece un nivel adicional de protección a los usuarios a través de Kaspersky Security Network. Este método de protección está diseñado para combatir amenazas persistentes avanzadas y ataques desde el día cero. Las tecnologías en la nube integradas y la experiencia de los analistas de virus de Kaspersky hacen que Kaspersky Endpoint Security sea una opción inigualable contra las amenazas de red más sofisticadas.

Podrá encontrar detalles sobre la protección mejorada de Kaspersky Endpoint Security en el sitio web de Kaspersky.

## Verificar si el punto de distribución opera como servidor proxy de KSN

Puede habilitar un servidor proxy de KSN en un dispositivo administrado asignado para funcionar como punto de distribución. Para funcionar como proxy de KSN, el dispositivo administrado debe tener activo el servicio ksnproxy. Puede verificar, activar o desactivar este servicio en el dispositivo localmente.

El dispositivo designado como punto de distribución puede utilizar Windows o Linux. El modo de llevar a cabo la verificación en el punto de distribución depende del sistema operativo instalado en el punto de distribución.

*Para comprobar si el punto de distribución basado en Windows está operando como servidor proxy de KSN:*

1. En el dispositivo de punto de distribución, en Windows, abra **Servicios** (**Todos los programas** → **Herramientas administrativas** → **Servicios**).
2. En la lista de servicios, verifique si el servicio ksnproxy se está ejecutando.

   Si el servicio ksnproxy se está ejecutando, entonces el Agente de red del dispositivo participa en Kaspersky Security Network y funciona como servidor proxy de KSN para los dispositivos administrados incluidos en el alcance del punto de distribución.

Si lo desea, puede desactivar el servicio ksnproxy. En este caso, el Agente de red del punto de distribución deja de participar en Kaspersky Security Network. Esto requiere derechos de administrador local.

*Para verificar si un punto de distribución con Linux opera como servidor proxy de KSN:*

1. En el dispositivo que actúe como punto de distribución, abra la lista de procesos en ejecución.
2. En la lista de procesos en ejecución, compruebe si `/opt/kaspersky/ksc64/sbin/ksnproxy` el proceso se está ejecutando.

Si el servicio ksnproxy se está ejecutando, entonces el Agente de red del dispositivo participa en Kaspersky Security Network y funciona como servidor proxy de KSN para los dispositivos administrados incluidos en el alcance del punto de distribución.

## Alternar entre la ayuda en línea y la ayuda sin conexión

Si no tiene acceso a Internet, puede utilizar la Ayuda sin conexión.

*Para cambiar entre la ayuda en línea y la ayuda sin conexión:*

1. En la ventana principal de Kaspersky Security Center, en el árbol de la consola, seleccione **Kaspersky Security Center 15.1**.
2. Haga clic en el vínculo **Configuración de interfaz global**.

   Se abre la ventana de configuración.
3. En la ventana de configuración, haga clic en **Utilice la Ayuda sin conexión**.
4. Haga clic en **Aceptar**.

El cambio se aplica y se guarda. Si lo desea, puede volver a cambiar la configuración en cualquier momento y comenzar a utilizar la Ayuda en línea en cualquier momento.

# Exportación de eventos a sistemas SIEM

Esta sección explica cómo exportar eventos registrados por Kaspersky Security Center a sistemas de Información de seguridad externa y Administración de eventos (SIEM).

## Configurar la exportación de eventos a sistemas SIEM

Kaspersky Security Center permite la configuración mediante uno de los siguientes métodos: exportar a cualquier sistema SIEM que utilice formato Syslog, exportar a los sistemas SIEM QRadar, Splunk y ArcSight que utilizan formatos LEEF y CEF o exportar eventos a sistemas SIEM directamente desde la base de datos de Kaspersky Security Center. Cuando complete este escenario, el Servidor de administración enviará los eventos al sistema SIEM automáticamente.

### Requisitos previos

Antes de configurar la exportación de eventos en Kaspersky Security Center, haga lo siguiente:

- Lea sobre los métodos disponibles para exportar eventos.
- Asegúrese de contar con los valores de la configuración del sistema.

Los pasos aquí descritos pueden realizarse en cualquier orden.

El proceso para exportar eventos a un sistema SIEM consiste de los siguientes pasos:

- **Configuración del sistema SIEM para que reciba eventos de Kaspersky Security Center**

  Instrucciones: Configurar la exportación de eventos en un sistema SIEM

- **Seleccionar eventos que desea exportar al sistema SIEM:**

  Instrucciones:

  - Consola de administración: Marcar eventos de una aplicación de Kaspersky para exportarlos en formato Syslog, Marcar eventos generales para que se los exporte en formato Syslog
  - Kaspersky Security Center Web Console: Marcar eventos de una aplicación de Kaspersky para que se los exporte en formato Syslog, Marcar eventos generales para que se los exporte en formato Syslog

- **Configuración de la exportación de eventos a sistemas SIEM mediante uno de los siguientes métodos:**

  - Mediante los protocolos TCP/IP, UDP o TLS sobre TCP

    Instrucciones:

    - Consola de administración: Configurar la exportación de eventos a sistemas SIEM
    - Kaspersky Security Center Web Console: Configurar la exportación de eventos a sistemas SIEM

  - Exporte los eventos directamente desde la base de datos de Kaspersky Security Center (la base de datos de Kaspersky Security Center proporciona un conjunto de vistas públicas, que se describen en el documento klakdb.chm).

### Resultados

Tras configurar la exportación de eventos al sistema SIEM, si marcó eventos como exportables, podrá ver los resultados de la exportación.

## Antes de comenzar

Al configurar la exportación automática de eventos en Kaspersky Security Center, debe especificar algunas de las configuraciones del sistema SIEM. Se recomienda que verifique estas configuraciones de antemano a fin de prepararse para configurar Kaspersky Security Center.

Para configurar correctamente el envío automático de eventos a un sistema SIEM, debe conocer los valores de los siguientes parámetros:

- **Dirección del servidor del sistema SIEM**

  La dirección IP del servidor en el que está instalado el sistema SIEM. Encontrará este valor en la configuración del sistema SIEM.

- **Puerto del servidor del sistema SIEM**

  El número de puerto usado para establecer una conexión entre Kaspersky Security Center y su servidor del sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center y en la configuración del destinatario de su sistema SIEM.

- **Protocolo**

  Protocolo usado para transferir mensajes de Kaspersky Security Center a su sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center y en la configuración del destinatario de su sistema SIEM.

# Acerca de los eventos en Kaspersky Security Center

Kaspersky Security Center le permite recibir información sobre los eventos de funcionamiento del Servidor de administración y aplicaciones de Kaspersky instaladas en dispositivos administrados. La información sobre estos eventos se guarda en la base de datos del Servidor de administración. Puede exportar esta información a un sistema SIEM externo. Al hacerlo, permitirá que los administradores del sistema SIEM respondan oportunamente a los sucesos del sistema de seguridad que se registren en dispositivos o grupos de dispositivos administrados.

## Tipos de evento

En Kaspersky Security Center existen los siguientes tipos de eventos:

- Eventos generales. Esta clase de evento ocurre en todas las aplicaciones de Kaspersky administradas. Un ejemplo de evento general es Brote de virus. Los eventos generales tienen una sintaxis y una semántica estrictamente definidas. Los eventos generales se utilizan en, por ejemplo, los paneles e informes.

- Eventos específicos de las aplicaciones de Kaspersky administradas. Cada aplicación de Kaspersky administrada tiene su propio conjunto de eventos.

### Orígenes de eventos

Los eventos pueden ser generados por las siguientes aplicaciones:

- Componentes de Kaspersky Security Center:
  - Servidor de administración
  - Agente de red
  - Servidor de MDM para iOS
- Aplicaciones administradas por Kaspersky

  Para obtener detalles sobre los eventos generados por las aplicaciones administradas por Kaspersky, consulte la documentación de la aplicación correspondiente.

Puede ver la lista completa de los eventos que puede generar una aplicación en la pestaña **Configuración de eventos** en la directiva de la aplicación. Para el Servidor de administración, también puede ver la lista de eventos en las propiedades del Servidor de administración.

### Nivel de importancia de los eventos

Cada evento tiene su propio nivel de importancia. El nivel de importancia que se le asigna a un evento puede variar según las circunstancias en las que ocurre. Existen cuatro niveles de importancia:

- Un *evento crítico* es un evento que se registra cuando ocurre un problema de extrema gravedad, que puede derivar en pérdidas de información, en un error crítico o en un fallo de funcionamiento.
- Un *error funcional* es un evento que se registra cuando ocurre un problema, fallo o error graves en el funcionamiento de la aplicación o en la ejecución de un procedimiento.
- Una *advertencia* es un evento que no necesariamente es grave, pero que anticipa un posible problema en el futuro. La mayoría de los eventos se catalogan como advertencias si, a pesar de que el evento haya ocurrido, la aplicación puede recuperarse sin sufrir una pérdida de información o de funcionalidad.
- Un evento *informativo* es un evento que se registra para informar que una operación o procedimiento se completaron sin errores o que la aplicación funciona correctamente.

Cada evento tiene un plazo de almacenamiento definido, durante el cual lo puede ver o modificar en Kaspersky Security Center. Algunos eventos no se guardan en la base de datos del Servidor de administración de forma predeterminada porque su plazo de almacenamiento está definido en cero. Para que un evento pueda exportarse, debe permanecer almacenado al menos un día en la base de datos del Servidor de administración.

## Acerca de la exportación de eventos

La exportación de eventos puede utilizarse en sistemas centralizados que permiten atender a los problemas de seguridad en un nivel organizativo y técnico. Estos sistemas, denominados sistemas SIEM, brindan servicios para hacer un monitoreo de la seguridad y son capaces de integrar la información de distintas soluciones. Pueden analizar, en tiempo real, los eventos y las alertas de seguridad que generan las aplicaciones, el hardware de red y los centros de operaciones de seguridad (SOC).

Los sistemas SIEM reciben información de muchas fuentes, como redes, soluciones de seguridad, servidores, aplicaciones y bases de datos. Pueden integrar los datos que obtienen para reducir las probabilidades de que un evento crítico pase desapercibido. También pueden realizar análisis automatizados de alertas y eventos correlacionados para notificar a los administradores de cualquier problema de seguridad inmediato. Las alertas de estos sistemas se pueden comunicar a través de un panel o tablero, o se pueden enviar por correo electrónico u otra vía provista por un tercero.

El proceso de exportación de eventos desde Kaspersky Security Center a sistemas SIEM externos involucra a dos partes: un remitente de eventos (Kaspersky Security Center) y un destinatario para los eventos (el sistema SIEM). Para exportar eventos correctamente, debe configurar estos parámetros en su sistema de SIEM y en la Consola de administración de Kaspersky Security Center. No importa cuál de los dos lados se configura primero. Puede configurar la transmisión de eventos en Kaspersky Security Center y luego configurar la recepción de estos por el sistema SIEM, o viceversa.

## Métodos para enviar eventos desde Kaspersky Security Center

Hay tres métodos para enviar eventos desde Kaspersky Security Center a los sistemas externos:

- El envío de eventos a través del protocolo de Syslog a cualquier sistema SIEM

  Usando el protocolo de Syslog, puede transmitir cualquier evento que ocurra en el Servidor de administración de Kaspersky Security Center y en Aplicaciones de Kaspersky instaladas en dispositivos administrados. El protocolo de Syslog es un protocolo de registro de mensajes estándares. Puede utilizarlo para exportar eventos a cualquier sistema SIEM.

  Para ello, debe marcar los eventos que desea transmitir al sistema SIEM. Puede marcar los eventos en Consola de administración o en Kaspersky Security Center Web Console. Solo los eventos marcados se transmitirán al sistema SIEM. Si no marcó nada, no se transmitirá ningún evento.

- Envío de eventos a través de los protocolos CEF y LEEF a sistemas de QRadar, Splunk y ArcSight

  Puede utilizar los protocolos CEF y LEEF para exportar eventos generales. Al exportar eventos a través de los protocolos CEF y LEEF, no tiene la posibilidad de seleccionar eventos específicos para exportarlos. En su lugar, se exportan todos los eventos generales. Para convertir eventos de Kaspersky Security Center a eventos en formato CEF y LEEF, debe utilizar el archivo siem_conversion_rules.xml. Este archivo contiene la lista de atributos de eventos de Kaspersky Security Center y los atributos correspondientes de eventos en formato CEF y LEEF. Además, el archivo siem_conversion_rules.xml contiene las reglas para generar mensajes correspondientes a eventos. Este archivo está incluido en el kit de distribución de Kaspersky Security Center.

  A diferencia del protocolo Syslog, los protocolos CEF y LEEF no son universales. CEF y LEEF están diseñados para los sistemas SIEM apropiados (QRadar, Splunk y ArcSight). Por lo tanto, cuando elige exportar eventos sobre uno de estos protocolos, usa el analizador requerido en el sistema SIEM.

- Directamente desde la base de datos de Kaspersky Security Center a cualquier sistema SIEM

  Este método de exportar eventos puede utilizarse para recibir eventos directamente de vistas públicas de la base de datos mediante consultas de SQL. Los resultados de una pregunta se guardan en un archivo de XML que se puede utilizar como datos de entrada para un sistema externo. Solo los eventos disponibles en vistas públicas se pueden exportar directamente desde la base de datos.

## Recepción de eventos por parte del sistema SIEM

El sistema SIEM debe recibir y correctamente analizar eventos recibidos de Kaspersky Security Center. Para que esto ocurra, el sistema SIEM debe estar correctamente configurado. El proceso de configuración depende del sistema SIEM que se utilice. Sin embargo, existen algunos pasos de configuración generales (como la configuración del receptor y el analizador) que son comunes a todos.

# Acerca de la configuración de la exportación de eventos en un sistema SIEM

El proceso de exportación de eventos desde Kaspersky Security Center a sistemas SIEM externos involucra a dos partes: un remitente de eventos (Kaspersky Security Center) y un destinatario para los eventos (el sistema SIEM). Debe configurar la exportación de eventos en su sistema SIEM y en Kaspersky Security Center.

Los ajustes que especifique en el sistema SIEM dependerán del sistema particular que esté utilizando. En general, para todo sistema SIEM, deberá configurar un receptor y, opcionalmente, un analizador que procese los eventos recibidos.

## Configuración del receptor

Para recibir eventos enviados por Kaspersky Security Center, debe configurar el destinatario en su sistema SIEM. Por lo general, deberá especificar los valores de los siguientes parámetros dentro del sistema SIEM:

- **Protocolo de exportación o tipo de entrada**

  Es el protocolo de transferencia de mensajes, por ejemplo, UDP. Este protocolo debe ser igual que el protocolo que especificó en Kaspersky Security Center.

- **Puerto**

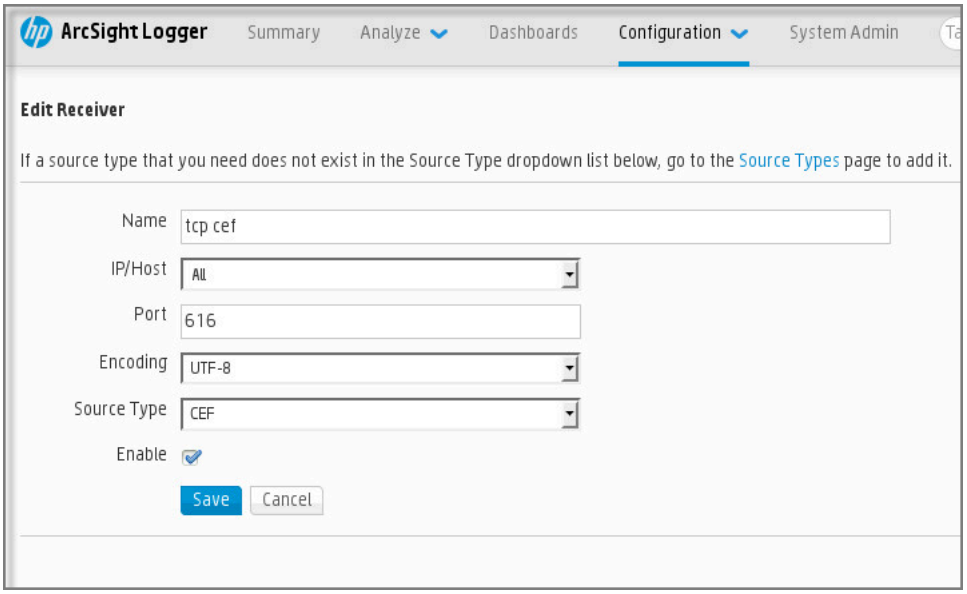
  Número de puerto utilizado para conectarse a Kaspersky Security Center. Este puerto debe ser igual que el puerto que especificó en Kaspersky Security Center.

- **Protocolo de mensajes o tipo de origen**

  El protocolo usado para exportar eventos al sistema SIEM. Puede ser uno de los protocolos estándares: Syslog, CEF o LEEF. El sistema SIEM selecciona el analizador sintáctico del mensaje según el protocolo que especifica.

Según el sistema SIEM que utilice, debería especificar algunas configuraciones adicionales del destinatario.

La figura siguiente muestra la pantalla de configuración del destinatario en ArcSight.




Configuración del destinatario en ArcSight

### Analizador sintáctico de mensajes

Los eventos exportados se transfieren al sistema SIEM en forma de mensajes. Estos mensajes deben analizarse; de lo contrario, el sistema SIEM no puede hacer uso de la información de los eventos. Los analizadores sintácticos de mensajes son parte del sistema SIEM; se usan para separar los contenidos del mensaje en los campos relevantes; por ejemplo, ID del evento, gravedad, descripción y parámetros. Esto permite al sistema SIEM procesar eventos recibidos de Kaspersky Security Center, de modo que se puedan almacenar en la base de datos del sistema SIEM.

## Marcar los eventos que se exportarán a un sistema SIEM en formato Syslog

Después de habilitar la exportación automática de eventos, debe seleccionar qué eventos se exportarán al sistema SIEM externo.

Para configurar la exportación de eventos en formato Syslog a un sistema externo, puede optar por una de estas vías:

- Marcar eventos generales. Si marca los eventos que desea exportar en la configuración de una directiva, en la configuración de los eventos o en la configuración del Servidor de administración, el sistema SIEM recibirá esos eventos cuando ocurran en cualquier aplicación sujeta a la directiva. Si los eventos exportados ya estaban seleccionados en la directiva, no podrá redefinirlos para una aplicación específica que esté administrada por esa directiva.

- Marcar eventos correspondientes a una aplicación administrada. Si marca eventos que correspondan a una aplicación administrada instalada en un dispositivo administrado, el sistema SIEM únicamente recibirá los eventos que ocurran en esa aplicación.

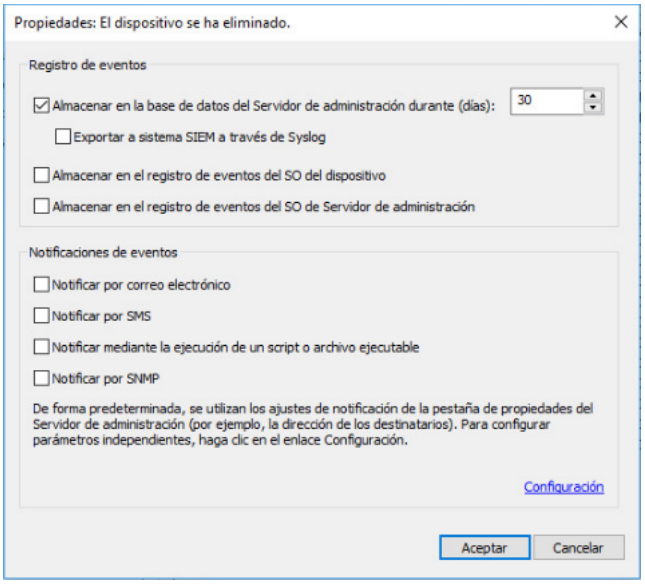
# Marcar eventos de una aplicación de Kaspersky para exportarlos en formato Syslog

Si desea exportar eventos que sucedan en una aplicación administrada de un dispositivo administrado, puede marcar esos eventos. Si ya se habían exportado eventos marcados en una directiva, no podrá redefinir esos eventos para una aplicación puntual que esté administrada por esa directiva.

*Para marcar los eventos de una aplicación administrada que se exportarán:*

1. En el árbol de consola de Kaspersky Security Center, seleccione el nodo **Dispositivos administrados** y vaya a la pestaña **Dispositivos**.
2. Haga clic con el botón derecho del ratón para abrir el menú contextual del dispositivo relevante y seleccione **Propiedades**.
3. En la ventana que se abre, que contendrá las propiedades del dispositivo, vaya a la sección **Aplicaciones**.
4. En la lista de aplicaciones que aparece, seleccione la aplicación cuyos eventos tiene que exportar y haga clic en el botón **Propiedades**.
5. En la ventana de propiedades de la aplicación, seleccione la sección **Configuración de eventos**.
6. En la lista de eventos que aparece, seleccione uno o varios eventos que se tienen que exportar al sistema SIEM, y hacer clic en el botón **Propiedades**.
7. En la ventana de propiedades del evento que aparece, seleccione la casilla **Exportar al sistema SIEM usando Syslog** para marcar los eventos seleccionados para exportar en formato Syslog. Anule la selección de la casilla **Exportar al sistema SIEM usando Syslog** para desmarcar los eventos seleccionados para exportar en formato Syslog.

   Si las propiedades del evento se definen en una directiva, los campos de esta ventana no se pueden modificar.




Ventana Propiedades de eventos

8. Haga clic en **Aceptar** para guardar los cambios.

9. Haga clic en **Aceptar** en la ventana de propiedades de aplicación y en la ventana de propiedades del dispositivo.

Los eventos marcados se enviarán al sistema SIEM en formato Syslog. Los eventos para los que anuló la selección de la casilla **Exportar al sistema SIEM usando Syslog** no se exportarán a un sistema SIEM. La exportación comenzará inmediatamente después de que habilite la exportación automática y seleccione los eventos para exportar. Configure el sistema SIEM para asegurarse de que pueda recibir eventos de Kaspersky Security Center.

## Marcar eventos generales para que se los exporte en formato Syslog

Si desea exportar eventos que ocurrieron en todas las aplicaciones administradas por una directiva específica, marque los eventos para exportar en la directiva. En este caso, no puede marcar eventos para una aplicación administrada en particular.

*Para marcar eventos generales y exportarlos a un sistema SIEM:*

1. En el árbol de consola de Kaspersky Security Center, seleccione el nodo **Directivas**.

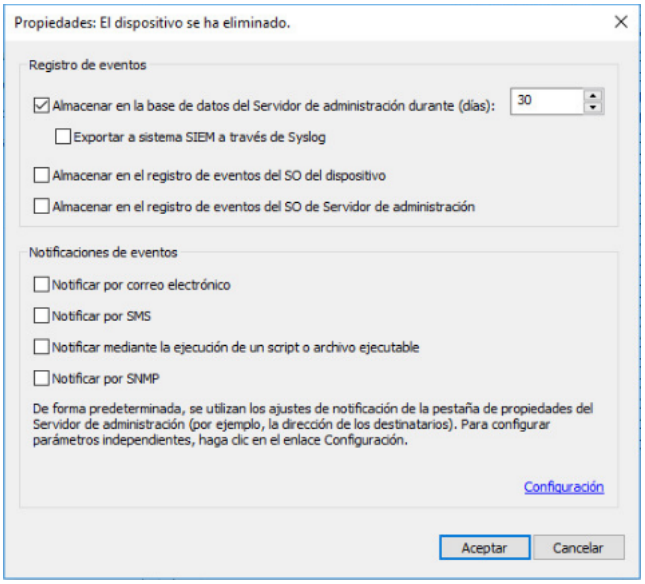
2. Haga clic con el botón derecho del ratón para abrir el menú contextual de la directiva relevante y seleccionar **Propiedades**.

3. En la directiva de las propiedades que se abre, seleccione la sección **Configuración de eventos**.

4. En la lista de eventos que aparece, seleccione uno o varios eventos que se tienen que exportar al sistema SIEM, y hacer clic en el botón **Propiedades**.

   Si tiene que seleccionar todos los eventos, haga clic en **Seleccionar todo**.

5. En la ventana de propiedades del evento que aparece, seleccione la casilla **Exportar al sistema SIEM usando Syslog** para marcar los eventos seleccionados para exportar en formato Syslog. Anule la selección de la casilla **Exportar al sistema SIEM usando Syslog** para desmarcar los eventos seleccionados para exportar en formato Syslog.




Ventana Propiedades del evento del Servidor de administración

6. Haga clic en **Aceptar** para guardar los cambios.

7. En la ventana de propiedades de la directiva, haga clic en **Aceptar**.

Los eventos marcados se enviarán al sistema SIEM en formato Syslog. Los eventos para los que anuló la selección de la casilla **Exportar al sistema SIEM usando Syslog** no se exportarán a un sistema SIEM. La exportación comenzará inmediatamente después de que habilite la exportación automática y seleccione los eventos para exportar. Configure el sistema SIEM para asegurarse de que pueda recibir eventos de Kaspersky Security Center.

# Acerca de la exportación de eventos en formato Syslog

Los eventos del Servidor de administración y los eventos de las aplicaciones de Kaspersky que se encuentran instaladas en los dispositivos administrados se pueden exportar a un sistema SIEM en formato Syslog.

Syslog es un protocolo de registro de mensajes estándar. Permite que el software que genera los mensajes, el sistema que los almacena y el software que los reporta y analiza sean entidades separadas. Cada mensaje se etiqueta con un código numérico que indica el tipo de software que lo ha generado. A cada mensaje se le asigna, además, un nivel de gravedad.

La definición del formato Syslog se encuentra publicada en documentos RFC del Grupo de Trabajo de Ingeniería de Internet o IETF (estándares de Internet). El estándar RFC 5424 es usado para exportar los eventos desde Kaspersky Security Center a sistemas externos.

En Kaspersky Security Center, puede configurar la exportación de eventos a sistemas externos usando el formato Syslog.

El proceso de exportación consta de dos pasos:

1. Habilitar la exportación de eventos automática. En este paso, Kaspersky Security Center se configura de modo que envíe eventos al sistema SIEM. Kaspersky Security Center empieza a enviar eventos inmediatamente después de que habilita la exportación automática.

2. Seleccionar los eventos que se exportarán al sistema externo. Este paso consiste en indicar cuáles eventos deberán exportarse al sistema SIEM.

# Acerca de la exportación de eventos en formato CEF o LEEF

Los eventos generales y los eventos que las aplicaciones de Kaspersky transfieren al Servidor de administración se pueden exportar al sistema SIEM en los formatos CEF y LEEF. El conjunto de eventos exportados se predefine, y no puede seleccionar los eventos que se exportarán. Antes de enviar eventos al sistema SIEM (QRadar, ArcSight o Splunk), es necesario interpretar los eventos de Kaspersky Security Center en eventos en formato CEF y LEEF mediante las reglas especificadas en el archivo siem_conversion_rules.xml.

Según el sistema SIEM que utilice, deberá elegir uno u otro formato de exportación. La siguiente tabla muestra los formatos correspondientes a algunos sistemas SIEM.

Formatos de exportación de eventos por sistema SIEM

| Sistema SIEM | Formato de exportación |
|---|---|
| QRadar | LEEF |
| ArcSight | CEF |
| Splunk | CEF |

- LEEF (Log Event Extended Format) es un formato de evento personalizado para IBM Security QRadar SIEM. QRadar puede integrar, identificar y procesar eventos LEEF. Los eventos LEEF deben usar la codificación de caracteres UTF-8. Puede encontrar la información detallada del protocolo LEEF en el Centro de conocimientos de IBM.

- CEF (Formato de eventos comunes) es un estándar abierto para la gestión de registros que mejora el interoperabilidad de la información relacionada con la seguridad desde diferentes dispositivos y aplicaciones de red y seguridad. CEF le permite usar un formato de registros de eventos común de modo que los datos se puedan integrar y agregarse fácilmente para el análisis por un sistema de gestión de la empresa. Los eventos CEF deben usar la codificación de caracteres UTF-8.

La exportación automática significa que Kaspersky Security Center envía eventos generales al sistema SIEM. La exportación automática de eventos se inicia inmediatamente después de que la habilita. Esta sección explica detalladamente cómo habilitar la exportación automática de eventos.

# Configurar Kaspersky Security Center para exportar eventos a un sistema SIEM

Puede habilitar la exportación automática de eventos en Kaspersky Security Center.

Solo se pueden exportar eventos generales desde las aplicaciones administradas mediante los formatos CEF y LEEF. Las reglas de interpretación utilizadas para convertir eventos a los formatos CEF y LEEF se especifican en el archivo siem_conversion_rules.xml que se incluye en el kit de distribución de Kaspersky Security Center. Los eventos específicos de la aplicación no se pueden exportar desde las aplicaciones administradas mediante los formatos CEF y LEEF. Si necesita exportar eventos de aplicaciones administradas o un conjunto personalizado de eventos que se haya configurado utilizando las directivas de aplicaciones administradas, debe exportar los eventos en formato Syslog.

*Para habilitar la exportación automática de eventos, haga lo siguiente:*

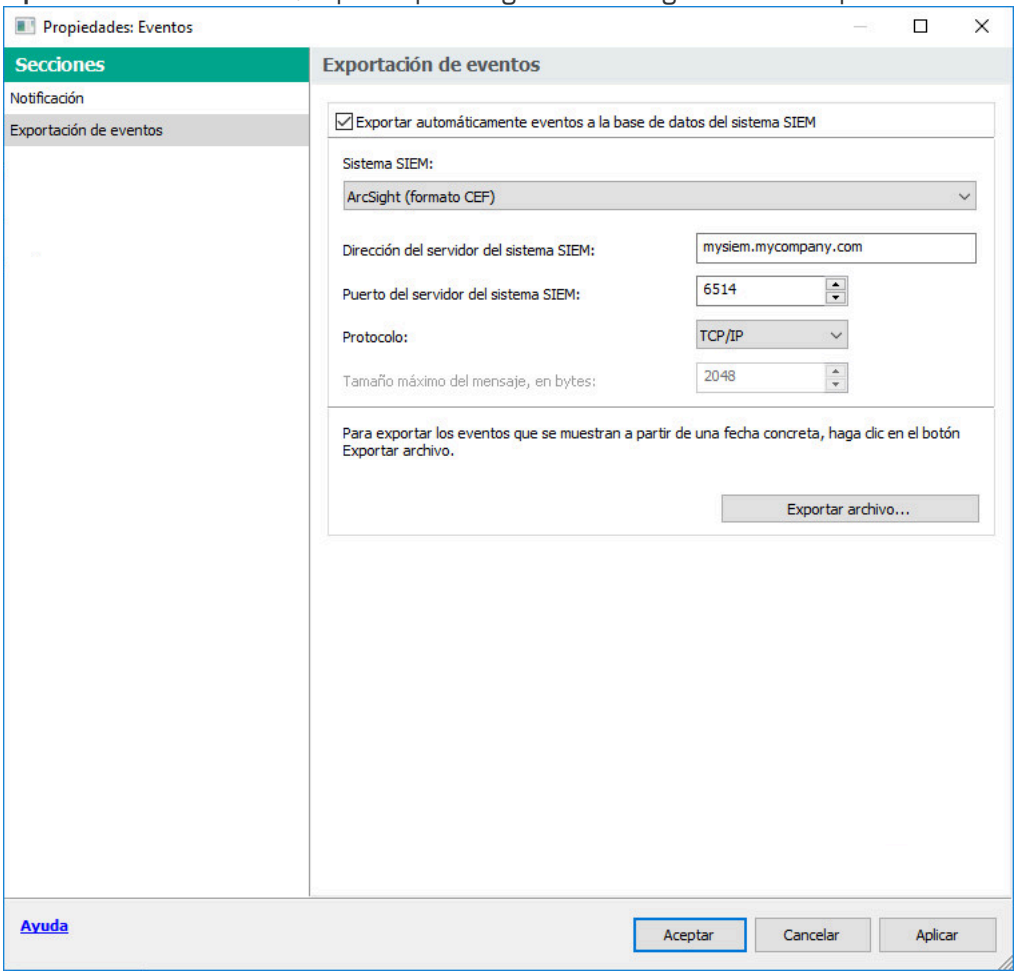
1. En el árbol de consola de Kaspersky Security Center, seleccione el Servidor de administración cuyos eventos desea exportar.

2. En el espacio de trabajo del Servidor de administración seleccionado, seleccione la pestaña **Eventos**.

3. Haga clic en la flecha desplegable junto al enlace **Configurar notificaciones y la exportación de eventos** y seleccione **Configurar la exportación al sistema SIEM** en la lista desplegable.

   Se abre la ventana propiedades de eventos, mostrando la sección **Exportación de eventos**.

4. En la sección **Exportación de eventos**, especifique la siguiente configuración de exportación:




Sección Exportación de evento de la ventana Propiedades del evento

- Exportar eventos a la base de datos del sistema SIEM automáticamente

  Seleccione esta casilla para habilitar la exportación automática de eventos al sistema SIEM. Cuando marque la casilla, se habilitarán todos los campos de la sección **Exportar eventos**.

- Sistema SIEM

  Seleccione el sistema SIEM al cual exportar los eventos: QRadar (formato LEEF), ArcSight (formato CEF), Splunk (formato CEF) y en formato Syslog (RFC 5424).

  Si selecciona el formato Syslog, debe especificar:

  Tamaño máximo de mensaje, bytes

  Especifique el tamaño máximo (en bytes) de un mensaje transmitido al sistema SIEM. Cada evento se transmite en un mensaje. Si la duración real de un mensaje supera el valor especificado, el mensaje es truncado y los datos se pueden perder. El tamaño predeterminado es de 2048 bytes. Este campo solo está disponible si seleccionara el formato de Syslog en el campo **Sistema SIEM**.

- Dirección del servidor del sistema SIEM

  Especifique la dirección del servidor del sistema SIEM. La dirección se puede especificar como un nombre NetBIOS o DNS o como una dirección IP.

- **Puerto del servidor del sistema SIEM**

  Especifique el número de puerto para conectarse con el servidor del sistema SIEM. Este número de puerto debe ser el mismo que el que usado por su sistema SIEM para recibir los eventos (consulte la sección Configuración de un sistema SIEM para más detalles).

- **Protocolo**

Seleccione el protocolo que se utilizará para transferir mensajes al sistema SIEM. Puede seleccionar los protocolos TCP, UDP o TLS sobre TCP.

Si selecciona el protocolo TLS sobre TCP, configure los siguientes ajustes:

- **Autenticación del servidor SIEM**

  Elija una de las siguientes formas de autenticar el servidor del sistema SIEM:

  - **Mediante el uso de certificados de CA**. Puede obtener un archivo con una lista de certificados de una entidad de certificación (también denominada "CA") de confianza y cargar ese archivo a Kaspersky Security Center. Kaspersky Security Center verificará si el certificado del servidor del sistema SIEM también fue firmado por una autoridad de certificación de confianza.

    Para agregar un certificado de confianza, haga clic en el botón **Examinar** y, a continuación, cargue el certificado.

    Si selecciona la opción **Mediante el uso de certificados de CA**, puede especificar los nombres de los sujetos en el campo **Sujetos de los certificados de servidor (opcional)**. Se denomina *Nombre del sujeto* al nombre de dominio para el que se ha obtenido un certificado. Para que Kaspersky Security Center pueda conectarse al servidor del sistema SIEM, el nombre de dominio del servidor del sistema SIEM debe aparecer como nombre del sujeto en el certificado del servidor del sistema SIEM. El servidor del sistema SIEM puede cambiar de nombre de dominio si modifica el nombre del sujeto en el certificado. Para ello, especifique los nombres de los sujetos en el campo **Sujetos de los certificados de servidor (opcional)**. Si alguno de los nombres de sujeto indicados en el campo coincide con el nombre de sujeto especificado en el certificado del sistema SIEM, Kaspersky Security Center considerará que el certificado es válido.

  - **Mediante el uso de huellas digitales SHA1 de certificados de servidor**. Puede agregar las huellas digitales SHA-1 de los certificados del sistema SIEM en Kaspersky Security Center. Si desea agregar una huella digital SHA-1, ingrésela en el campo ubicado bajo la opción.

- **Autenticación del cliente**

  Para la autenticación del cliente, puede utilizar su propio certificado o generar uno en Kaspersky Security Center.

  - **Insertar certificado**. Puede utilizar un certificado obtenido de cualquier fuente (por ejemplo, de una entidad de certificación de confianza). Para insertar un certificado existente, haga clic en el botón **Buscar certificado**. En la ventana **Certificado** abierta, elija uno de los siguientes tipos de certificado y, a continuación, especifique el certificado y su clave privada:

    - **Certificado X.509**Certificado X-509: Cargue el archivo que contenga la clave privada en el campo **Clave privada (*.prk, *.pem)** y el archivo que contenga el certificado en el campo **Certificado (*.cer)**. Para hacer esto, haga clic en el botón **Examinar** a la derecha del campo correspondiente y agregue el archivo requerido. Los archivos no dependen el uno del otro y no importa el orden en que se los carga. Tras cargar ambos archivos, ingrese la contraseña para decodificar la clave privada en el campo **Contraseña**. Si la clave privada no está codificada, puede dejar la contraseña en blanco.

    - **Contenedor PKCS #12**. Use el campo **Archivo del certificado** para cargar un único archivo que contenga tanto el certificado como su clave privada. Para hacer esto, haga clic en el botón **Examinar** a la derecha del campo y luego agregue el archivo requerido. Tras cargar el archivo, ingrese la contraseña para decodificar la clave privada en el campo **Contraseña**. Si la clave privada no está codificada, puede dejar la contraseña en blanco.

  - **Generar clave**. Puede generar un certificado autofirmado dentro de Kaspersky Security Center. Haga clic en el botón **Generar certificado** y, a continuación, introduzca un nombre de asunto en el campo **Sujeto**. El certificado de cliente se genera para este nombre de sujeto y la huella digital SHA-1 de este certificado aparece en el campo **Huella digital SHA1 del certificado de cliente**. El certificado autofirmado que se genere quedará almacenado en Kaspersky Security Center, y usted podrá transferir la parte pública del certificado o su huella digital SHA-1 al sistema SIEM.

5. Si desea exportar a la base de datos del sistema SIEM los eventos que ocurrieron después de una fecha especificada en el pasado, haga clic en el botón **Exportar archivo** y especifique la fecha de inicio para la exportación del evento. De forma predeterminada, la exportación del evento inicia inmediatamente después de que la habilita.

6. Para comprobar que la conexión con el sistema SIEM esté configurada correctamente, haga clic en el botón **Probar configuración**.

   La aplicación intenta establecer conexión con el servidor del sistema SIEM y enviar un evento de prueba. Si no se establece la conexión, se muestra un mensaje de error. Si se establece la conexión, no se muestra ningún mensaje. Puede ver el evento de prueba en la pestaña **Eventos**, si es necesario.

7. Haga clic en **Aceptar**.

La exportación automática de eventos está habilitada.

Después de habilitar la exportación automática de eventos, debe seleccionar qué eventos se exportarán al sistema SIEM.

# Exportación de eventos directamente desde la base de datos

Puede recuperar eventos directamente desde la base de datos de Kaspersky Security Center sin necesidad de usan la interfaz de Kaspersky Security Center. Puede consultar directamente las vistas públicas y recuperar los datos del evento o crear su propia vista a partir de vistas públicas existentes y dirigirse a ellas para obtener los datos que necesita.

## Vistas públicas

Para su conveniencia, un conjunto de vistas públicas se proporciona en la base de datos de Kaspersky Security Center. Puede encontrar la descripción de estas vistas públicas en el documento klakdb.chm.

La vista pública v_akpub_ev_event contiene un conjunto de campos que representan los parámetros del evento en la base de datos. En el documento klakdb.chm, también puede encontrar información sobre las vistas públicas correspondiente a otras entidades de Kaspersky Security Center; por ejemplo, dispositivos, aplicaciones o usuarios. Puede usar esta información en sus consultas.

Esta sección contiene instrucciones para ejecutar una consulta SQL mediante la utilidad klsql2 y un ejemplo de consulta.

Para crear consultas SQL o vistas de bases de datos, también puede utilizar cualquier otro programa para trabajar con bases de datos. En la sección correspondiente, se proporciona información sobre cómo ver los parámetros para conectar a la base de datos de Kaspersky Security Center, como el nombre de la instancia y nombre de la base de datos.

# Ejecución de una consulta SQL con la utilidad klsql2

En este artículo se describe cómo descargar y usar la utilidad klsql2, y cómo ejecutar una consulta SQL con esta utilidad.

*Para usar la utilidad klsql2:*

1. Inicie la utilidad klsrvswch desde la carpeta de instalación de Kaspersky Security Center. La ruta de instalación predeterminada es <Disk>:\Archivos de programa(x86)\Kaspersky Lab\Kaspersky Security Center. No utilice versiones de la utilidad klsql2 diseñadas para versiones anteriores de Kaspersky Security Center.

2. Cree un archivo con la extensión src.sql en cualquier editor de texto y póngalo en la misma carpeta que la utilidad.

3. En el archivo .sql creado, escriba la consulta SQL que desea, y luego, guarde el archivo.

4. En el dispositivo que tiene instalado el Servidor de administración de Kaspersky Security Center, en la línea de comandos, escriba el siguiente comando para ejecutar la consulta SQL desde el archivo .sql y guardar los resultados en el archivo result.xml:

   ```
   klsql2 -i src.sql -u < nombre de usuario > -p < contraseña > -o result.xml
   ```

   dónde < `nombre de usuario` > y < `contraseña` > son credenciales de la cuenta de usuario que tiene acceso a la base de datos.

5. Si es necesario, ingrese el nombre de usuario y la contraseña de la cuenta de usuario que tiene acceso a la base de datos.

6. Abra los archivos result.xml creados recientemente para ver los resultados de la consulta SQL.

Puede modificar el archivo .sql y crear cualquier consulta SQL para las vistas públicas. A continuación, desde la línea de comandos, ejecute su consulta SQL y guarde los resultados en un archivo.

## Ejemplo de una consulta de SQL usando la utilidad klsql2

Esta sección muestra un ejemplo de una consulta SQL, ejecutada por medio de la utilidad klsql2.

Los ejemplos siguientes ilustran la recuperación de eventos que ocurrieron en dispositivos durante los siete días anteriores, y muestran los eventos según la hora en la que se producen. Los eventos más recientes se muestran primero.

Ejemplo para Microsoft SQL Server:

```
SELECT
  /* identificador del evento */
  e.nId,

  /* hora en la que ocurrió el evento */
  e.tmRiseTime,

  /* nombre interno del tipo de evento */
  e.strEventType,

  /* nombre mostrado del evento */
  e.wstrEventTypeDisplayName,

  /* descripción mostrada del evento */
  e.wstrDescription,

  /* nombre del grupo donde se encuentra el dispositivo */
  e.wstrGroupName,

  /* nombre mostrado del dispositivo en el que ocurrió el evento */
  h.wstrDisplayName,
  CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

  /* Dirección IP del dispositivo en el que ocurrió el evento */
  CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
  INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Ejemplo para PostgreSQL:

```
SELECT
  /* identificador del evento */
  "e"."nId",

  /* hora en que ocurrió el evento */
  "e"."tmRiseTime",

  /* nombre interno del tipo de evento */
  "e"."strEventType",

  /* nombre mostrado del evento */
  "e"."wstrEventTypeDisplayName",

  /* descripción mostrada del evento */
  "e"."wstrDescription",

  /* descripción mostrada del evento */
  "e"."wstrGroupName",

  /* nombre mostrado del dispositivo en el que ocurrió el evento */
  "h"."wstrDisplayName",
  (
    CAST(("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST(("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST(("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* Dirección IP del dispositivo en el que ocurrió el evento */
    CAST(("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

Ejemplo para MySQL o MariaDB

```
SELECT

  /* identificador del evento */
  `e`.`nId`,

  /* hora en que ocurrió el evento */
  `e`.`tmRiseTime`,

  /* nombre interno del tipo de evento */
  `e`.`strEventType`,

  /* nombre mostrado del evento */
  `e`.`wstrEventTypeDisplayName`,

  /* descripción mostrada del evento */
  `e`.`wstrDescription`,

  /* nombre del grupo del dispositivo */
  `e`.`wstrGroupName`,

  /* nombre mostrado del dispositivo en el que ocurrió el evento */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* Dirección IP del dispositivo en el que ocurrió el evento */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

## Visualización del nombre de la base de datos de Kaspersky Security Center

Conocer el nombre de una base de datos puede ser útil en algunos casos (por ejemplo, si necesita enviar una consulta SQL y conectarse a la base de datos con un editor de scripts SQL).

*Para ver el nombre de la base de datos de Kaspersky Security Center:*

1. En el árbol de la consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y seleccione **Propiedades**.

2. En la ventana de propiedades del Servidor de administración, en el panel Secciones, seleccione **Avanzado** y a continuación **Detalles de la base de datos actual**.

3. En la sección **Detalles de la base de datos actual**, tenga en cuenta las siguientes propiedades de la base de datos (ver figura a continuación):

- **Nombre de la instancia**

  Nombre de la instancia de base de datos de Kaspersky Security Center actual. El valor predeterminado es *.\KAV_CS_ADMIN_KIT*.

- **Nombre de la base de datos**

  Nombre de la base de datos de SQL de Kaspersky Security Center. El valor predeterminado es *KAV*.

- **Espacio para la base de datos de Kaspersky Security Center**

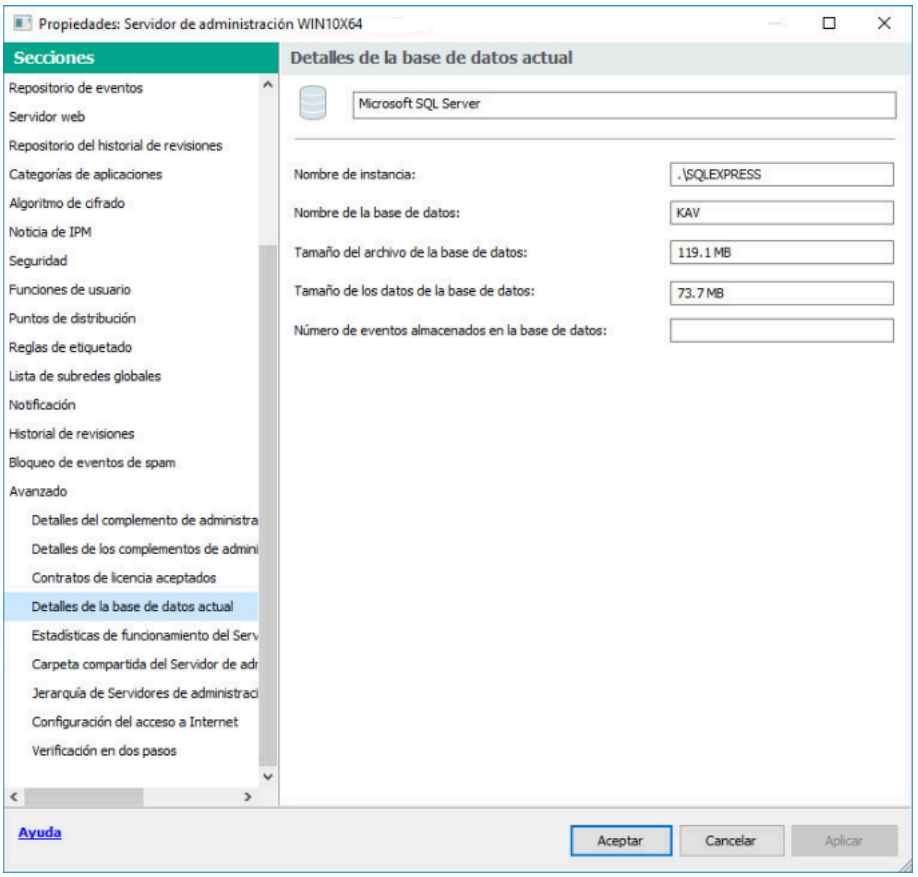
  El tamaño del archivo de base de datos. Si desea limpiar datos innecesarios, configure la compresión de las bases de datos mediante la tarea *Mantenimiento del Servidor de administración*.

- **Cantidad de datos en toda la base de datos**

  El tamaño real de los datos utilizados actualmente en el DBMS. El siguiente artículo describe cómo diagnosticar el DBMS: El tamaño de las bases de datos excede el límite.

- **Cantidad de eventos almacenados en la base de datos**

Cantidad de eventos almacenados en el DBMS. Consulte el siguiente artículo para obtener más detalles: Procesamiento y almacenamiento de eventos.




Sección con información sobre la base de datos actual del Servidor de administración

4. Haga clic en el botón **Aceptar** para cerrar la ventana de propiedades del Servidor de administración.

Use el nombre de la base de datos para dirigirse a la base de datos en sus consultas de SQL.

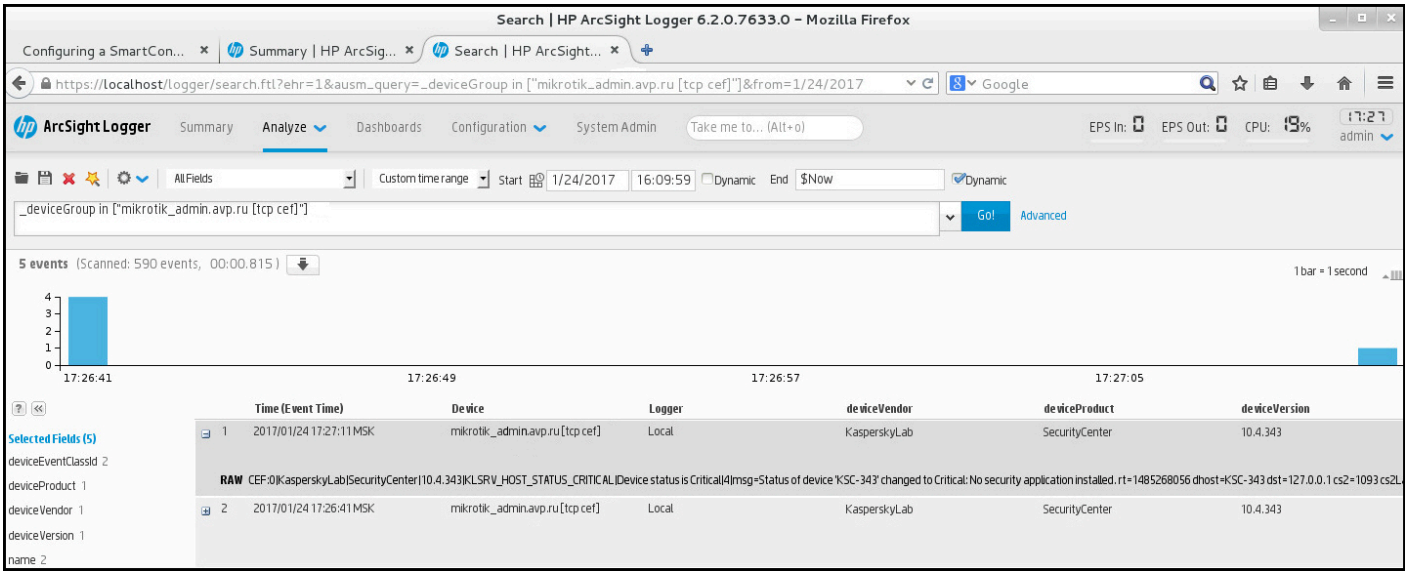
# Ver los resultados de la exportación

Puede controlar si el procedimiento de exportación de eventos se ha completado debidamente. Para ello, verifique si el sistema SIEM recibe mensajes con los eventos exportados.

Si los eventos enviados desde Kaspersky Security Center se reciben y analizan correctamente en su sistema SIEM, la configuración a ambos lados se realizó correctamente. De lo contrario, verifique la configuración que especificó en Kaspersky Security Center en comparación con la configuración en su sistema SIEM.

La imagen de más abajo muestra los eventos exportados a ArcSight. El primero de ellos, *Device status is Critical*, es un evento crítico del Servidor de administración que se refiere al estado de un dispositivo.

La representación de los eventos exportados a un sistema SIEM varía según el sistema SIEM utilizado.




Ejemplo de eventos

# Usar SNMP para enviar estadísticas a aplicaciones de terceros

Esta sección describe cómo obtener información del Servidor de administración mediante el Protocolo simple de administración de redes (SNMP) en Windows. Kaspersky Security Center contiene un agente SNMP, que transfiere estadísticas del rendimiento del Servidor de administración a las aplicaciones secundarias que utilizan DOI.

Esta sección también contiene información sobre cómo resolver problemas que puede encontrar al usar SNMP para Kaspersky Security Center.

## Configuración del servicio SNMP para usar con Kaspersky Security Center

En esta sección, se describe cómo configurar el servicio SNMP en Windows para obtener información del Servidor de administración mediante el Protocolo simple de administración de redes (SNMP).

La compatibilidad con SNMP está deshabilitada de forma predeterminada en Windows.

*Para habilitar la compatibilidad con SNMP en Windows, realice los siguientes pasos:*

1. Navegue al **Panel de control**.
2. Abra el menú **Agregar o quitar programas**.
3. Haga clic en **Activar o desactivar las funciones de Windows**.
4. En la lista de funciones de Windows, navegue a la función SNMP y haga clic en **Aceptar**.
5. Vaya a **Panel de control** → **Herramientas administrativas** → **Servicios**.

6. Elija el **Servicio SNMP** y ejecútelo.

7. Use `netstat` para comprobar se se está monitoreando un puerto UPD estándar.

La compatibilidad con SNMP se habilitará en Windows.

*Para configurar los servicios SNMP en Windows, realice los siguientes pasos:*

1. Asegúrese de que el componente **Agente SNMP** de Kaspersky Security Center se haya instalado durante la instalación normal o silenciosa.

2. Asegúrese de que el **Servicio SNMP** y los servicios de **Captura de SNMP** de Windows se estén ejecutando.

3. Asegúrese de que el navegador de MIB de ManageEngine esté instalado en su sistema.

4. En las propiedades del **Servicio SNMP**, en la pestaña **Seguridad**, agregue dos comunidades con los siguientes derechos:

| Comunidad | Derechos |
|---|---|
| `kaspersky` | `NOTIFY` |
| `public` | `READ WRITE` |

5. En el campo **Aceptar paquetes SNMP de estos hosts**, agregue la dirección IP del dispositivo donde está instalado el navegador de MIB de ManageEngine, por ejemplo, 10.10.10.105.

6. En la pestaña **Capturas**, escriba `kaspersky` en el campo **Nombre de la comunidad**.

7. Haga clic en **Aceptar** para guardar los cambios y cierre la ventana de propiedades del servicio.

8. En el navegador de MIB de ManageEngine, cargue el archivo adminkit.mib desde la carpeta de instalación de Kaspersky Security Center. De manera predeterminada, el archivo adminkit.mib se encuentra en la carpeta <Disco>:\Archivos de programa\Kaspersky Lab\Kaspersky Security Center\snmp.

9. En el campo **Host** de la ventana del navegador de MIB de ManageEngine, agregue la dirección IP del dispositivo donde está instalado el Servidor de administración de Kaspersky Security Center.

El servicio SNMP está configurado para obtener información del Servidor de administración mediante el Protocolo simple de administración de redes (SNMP).

# Agentes SNMP e identificadores de objetos

Para Kaspersky Security Center, el agente SNMP se implementa como una biblioteca dinámica `klsnmpag.dll]].dll`, que el instalador registra durante la instalación del Servidor de administración. El agente SNMP funciona dentro del proceso `[[snmp.exe` (que es un servicio de Windows). Las aplicaciones de terceros usan SNMP para recibir estadísticas (que vienen en forma de contadores) sobre el rendimiento del Servidor de administración.

Cada contador tiene un *identificador de objeto* único (también denominado DOI). Un identificador de objeto es una secuencia de números dividida por puntos. Los identificadores de objeto del Servidor de administración comienzan con el prefijo 1.3.6.1.4.1.23668.1093. El DOI del contador es una concatenación de ese prefijo con un sufijo que describe el contador. Por ejemplo, el contador con el valor DOI de 1.3.6.1.4.1.23668.1093.1.1.4 tiene el sufijo con el valor de 1.1.4.

Puede usar un cliente SNMP (como Zabbix) para supervisar el estado de su sistema. Para obtener la información, puede buscar un valor de DOI que corresponda a la información e ingresar ese valor en su cliente SNMP. Entonces, su cliente SNMP le devolverá otro valor que caracteriza el estado de su sistema.

La lista de contadores y tipos de contadores se encuentra en el archivo `adminkit.mib` del Servidor de administración. *MIB* son las siglas de Management Information Base. Puede importar y analizar archivos `.mib` a través de la aplicación MIB Viewer que está diseñada para solicitar y mostrar los valores del contador.

# Obtener un nombre de contador de serie a partir de un identificador de objeto

Para utilizar un identificador de objeto (DOI) para transferir información a aplicaciones de terceros, es posible que deba obtener un nombre de contador de serie de ese DOI.

*Para obtener un nombre de contador de serie de un DOI:*

1. Abra el archivo `adminkit.mib`, que se encuentra en el Servidor de administración, en un editor de texto.
2. Busque el espacio de nombres que describe el primer valor (de izquierda a derecha).

   Por ejemplo, para el sufijo DOI 1.1.4, sería `"counters" (::= { kladminkit 1 })`.
3. Busque el espacio de nombres que describe el segundo valor.

   Por ejemplo, para el sufijo 1.1.4 OID sería `counters 1`, que significa el `deployment`.
4. Busque el espacio de nombres que describe el tercer valor.

   Por ejemplo, para el sufijo OID 1.1.4 sería el `deployment 4`, que significa `hostsWithAntivirus`.

El nombre del contador de serie es la concatenación de estos valores, por ejemplo, `<MIB base namespace>.counters.deployment.hostsWithAntivirus`, y corresponde al DOI con el valor de 1.3.6.1.4.1.23668.1093.1.1.4.

# Valores de identificadores de objetos para SNMP

La siguiente tabla muestra los valores y descripciones de los identificadores de objetos (también conocidos como DOI) que se utilizan para transferir información sobre el rendimiento del Servidor de administración a aplicaciones de terceros.

| Valor del identificador de objeto | Tipo de datos numéricos | DOI | Descripción |
|---|---|---|---|
| deploymentStatus | INTEGER { ok(0), info(1), warning(2), critical(3) } | .1.3.6.1.4.1.23668.1093.1.1.1 | Estado de despliegue. El estado puede ser uno de los siguientes:<br>• **Información**. La licencia ya no es válida para N dispositivos.<br>• **Advertencia**. Uno de los siguientes:<br>Hay M equipos con aplicaciones de Kaspersky instaladas en un total de N dispositivos en grupos de Servidores de administración (N > M).<br>La licencia L caducará en N dispositivos en M días.<br>La tarea T de instalar aplicaciones se realizó correctamente en N dispositivos. Es necesario reiniciar M dispositivos.<br>• **Crítico**. Licencia caducó para N dispositivos.<br>• **Entendido**. Ninguna de las anteriores. |
| noAntivirusSoftware | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.1.2.1 | El motivo deploymentStatus muestra que el grupo de Servidores de administración contiene demasiados dispositivos sin aplicaciones administradas.<br>El valor será igual a 1 en caso de que algunos dispositivos se encuentren sin aplicaciones administradas. En caso contrario, el valor será igual a 0. |
| remoteInstallTaskFailed | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.1.2.2 | El motivo deploymentStatus muestra que la tarea de la instalación remota ha fallado en algunos dispositivos. Puede obtener el número de esos dispositivos a través de hostsRemoteInstallFailed. |
| licenceExpiring | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.1.2.3 | La razón por la cual deploymentStatus muestra que hay algunos dispositivos con una licencia que caduca en los próximos 7 días. Puede obtener el número de esos dispositivos a través de hostsLicenseExpiring. |
| licenceExpired | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.1.2.4 | La razón por la cual deploymentStatus muestra que hay algunos dispositivos con licencia vencida. Puede obtener el número de esos dispositivos a través de hostsLicenseExpired. |
| hostsInGroups | Counter32 | .1.3.6.1.4.1.23668.1093.1.1.3 | Número de dispositivos en los grupos del Servidor de administración. |
| hostsWithAntivirus | Counter32 | .1.3.6.1.4.1.23668.1093.1.1.4 | Número de dispositivos en los grupos del Servidor de administración con aplicaciones administradas instaladas. |
| hostsRemoteInstallFailed | Counter32 | .1.3.6.1.4.1.23668.1093.1.1.5 | Número de dispositivos en los que falló la tarea de instalación remota. |
| licenceExpiringSerial | OCTET STRING | .1.3.6.1.4.1.23668.1093.1.1.6 | Identificación de una clave de licencia que caduca pronto (en menos de 7 días). |
| licenceExpiredSerial | OCTET STRING | .1.3.6.1.4.1.23668.1093.1.1.7 | Identificación de la clave de licencia caducada. |
| licenceExpiringDays | Unsigned32 | .1.3.6.1.4.1.23668.1093.1.1.8 | Número de días antes de que caduque una licencia. Para este parámetro, el plazo de la licencia se considera caducado cuando quedan menos de siete días hasta la fecha de caducidad.<br>Si restan más de siete días para la fecha de caducidad, el valor es 0. |
| hostsLicenceExpiring | Counter32 | .1.3.6.1.4.1.23668.1093.1.1.9 | Número de dispositivos con una licencia que caduca pronto (en menos de 7 días). |
| hostsLicenceExpired | Counter32 | .1.3.6.1.4.1.23668.1093.1.1.10 | Número de dispositivos con licencia caducada. |

| Valor del identificador de objeto | Tipo de datos numéricos | DOI | Descripción |
|---|---|---|---|
| `updatesStatus` | `INTEGER { ok(0), info(1), warning(2), critical(3) }` | .1.3.6.1.4.1.23668.1093.1.2.1 | Estado actual de la actualización de las bases antivirus. El estado puede ser uno de los siguientes:<br>• **Información**. Las bases antivirus del Servidor de administración o de los dispositivos no se actualizan desde hace más de 1 día, y pasó menos de 1 día desde la instalación de la aplicación.<br>• **Advertencia**. Las bases antivirus del Servidor de administración o de los dispositivos no se actualizan desde hace más de 3 días. Este valor se puede cambiar en la configuración de grupo.<br>• **Crítico**. Las bases antivirus del Servidor de administración o de los dispositivos no se actualizan desde hace más de 7 días. Este valor se puede cambiar en la configuración de grupo.<br>• **Entendido**. Ninguna de las anteriores. |
| `serverNotUpdated` | `INTEGER { off(0), on(1) }` | .1.3.6.1.4.1.23668.1093.1.2.2.1 | Esto muestra que el Servidor de administración no se actualizó durante un tiempo de registro. La cantidad de tiempo que se considera larga se especifica en `updatesStatus`. |
| `notUpdatedHosts` | `INTEGER { off(0), on(1) }` | .1.3.6.1.4.1.23668.1093.1.2.2.2 | Esto muestra que algunos dispositivos no se actualizaron durante mucho tiempo (de manera predeterminada, 7 días o más para que sean **Crítico** y 3 días para recibir una **Advertencia**). Puede obtener el número de esos dispositivos a través de `hostsNotUpdated`. |
| `lastServerUpdateTime` | `OCTET STRING` | .1.3.6.1.4.1.23668.1093.1.2.3 | Última vez que se actualizaron las bases de antivirus en el Servidor de administración. |
| `hostsNotUpdated` | `Counter32` | .1.3.6.1.4.1.23668.1093.1.2.4 | Número de dispositivos que contienen bases antivirus que no se actualizan durante mucho tiempo (de manera predeterminada, 7 días o más para que sean **Crítico** y 3 días para recibir una **Advertencia**). Si hay dispositivos con el estado de actualización **Crítico**, solo se cuentan estos dispositivos. Puede obtener el estado de la actualización a través de `updatesStatus`. |
| `protectionStatus` | `INTEGER { ok(0), warning(2), critical(3) }` | .1.3.6.1.4.1.23668.1093.1.3.1 | Estado de protección en tiempo real. Uno de los siguientes:<br>• **Advertencia**. Uno de los siguientes:<br>Se ha detectado una brecha de seguridad en un dispositivo que pertenece al grupo de Servidores de administración.<br>Los errores de cifrado hicieron que algunos dispositivos cambiaran el estado de protección.<br>El análisis completo no se ha realizado en mucho tiempo.<br>• **Crítico**. La protección antivirus no funciona en algunos dispositivos de los grupos de Servidores de administración.<br>• **Entendido**. Ninguna de las anteriores. |
| `antivirusNotRunning` | `INTEGER { off(0), on(1) }` | .1.3.6.1.4.1.23668.1093.1.3.2.1 | Esto muestra que una aplicación de seguridad no se está ejecutando en algunos dispositivos. Puede obtener el número de esos dispositivos a través de `hostsAntivirusNotRunning`. |
| `realtimeNotRunning` | `INTEGER { off(0), on(1) }` | .1.3.6.1.4.1.23668.1093.1.3.2.2 | Esto muestra que la protección en tiempo real no se está ejecutando en algunos dispositivos. Puede obtener el número de esos dispositivos a través de `hostsRealtimeNotRunning`. |
| `notCuredFound` | `INTEGER { off(0), on(1) }` | .1.3.6.1.4.1.23668.1093.1.3.2.4 | Esto muestra que hay dispositivos que contienen objetos no desinfectados. Puede obtener el número de esos dispositivos a través de `hostsNotCuredObject`. |
| `tooManyThreats` | `INTEGER { off(0), on(1) }` | .1.3.6.1.4.1.23668.1093.1.3.2.5 | Esto muestra que se han encontrado amenazas en algunos dispositivos. Puede obtener el número de esos dispositivos a través de `hostsTooManyThreats`. |

| Valor del identificador de objeto | Tipo de datos numéricos | DOI | Descripción |
|---|---|---|---|
| virusOutbreak | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.6 | Esto muestra el estado del brote de virus del sistema.<br>El valor es igual a 1 si se encontró cierta cantidad de virus durante un determinado período de tiempo y 0 en caso contrario. La cantidad de virus y la cantidad de tiempo se especifican en el Servidor de administración mediante la configuración de `ataque de virus`. |
| hostsAntivirusNotRunning | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.3 | Número de dispositivos con aplicaciones de seguridad que no se están ejecutando. |
| hostsRealtimeNotRunning | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.4 | Número de dispositivos con protección en tiempo real que no se está ejecutando. |
| hostsRealtimeLevelChanged | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.5 | Número de dispositivos con un nivel de protección en tiempo real inaceptable. |
| hostsNotCuredObject | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.6 | Número de dispositivos que contienen objetos no desinfectados. |
| hostsTooManyThreats | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.7 | Número de dispositivos que contienen amenazas. |
| fullscanStatus | INTEGER { ok(0), info(1), warning(2), critical(3) } | .1.3.6.1.4.1.23668.1093.1.4.1 | Estado del análisis completo del antivirus. Uno de los siguientes:<br>• **Información**. Han pasado menos de 7 días desde el momento de la instalación de la aplicación.<br>• **Advertencia**. El análisis completo del antivirus no se ha realizado durante más de 7 días desde el momento de la instalación de la aplicación.<br>• **Crítico**. El análisis completo del antivirus no se ha realizado durante más de 14 días desde el momento de la instalación de la aplicación.<br>• **Entendido**. Ninguna de las anteriores. |
| notScannedLately | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.4.2.1 | Esto muestra que algunos dispositivos no se han analizado durante un cierto período de tiempo. Puede obtener el número de esos dispositivos a través de `hostsNotScannedLately`. La cantidad de tiempo se especifica en `fullScanStatus`. |
| hostsNotScannedLately | Counter32 | .1.3.6.1.4.1.23668.1093.1.4.3 | Número de dispositivos que no se han analizado durante un tiempo determinado. La cantidad de tiempo se especifica en `fullScanStatus`. |
| logicalNetworkStatus | INTEGER { ok(0), warning(1), critical(2) } | .1.3.6.1.4.1.23668.1093.1.5.1 | Estado de la red lógica del Servidor de administración. Uno de los siguientes:<br>• **Advertencia**. Si no se puede acceder al estado de advertencia de algún dispositivo o si hay dispositivos que no pertenecen a ningún grupo de Servidores de administración.<br>• **Crítico**. Si el Servidor de administración pierde control sobre algún dispositivo, o existen dispositivos en estado crítico a los que no se puede acceder.<br>• **Entendido**. Ninguna de las anteriores. |
| notConnectedLongTime | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.5.2.1 | Esto muestra que algunos dispositivos no han estado conectados al Servidor de administración durante mucho tiempo (7 días o más para un dispositivo en estado de **Advertencia** y 4 días para un dispositivo en estado **Crítico** ). Puede obtener el número de esos dispositivos a través de `hostsNotConnectedLongTime`. |
| controlLost | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.5.2.2 | Esto muestra que el Servidor de administración ha perdido del control sobre algún dispositivo. Puede obtener el número de esos dispositivos a través de `hostsControlLost`. |
| hostsFound | Counter32 | .1.3.6.1.4.1.23668.1093.1.5.3 | Número de dispositivos encontrados por el Servidor de administración que no pertenecen a ningún grupo de administración. |
| groupsCount | Counter32 | .1.3.6.1.4.1.23668.1093.1.5.4 | Número de grupos de administración en el Servidor de administración. |

| Valor del identificador de objeto | Tipo de datos numéricos | DOI | Descripción |
|---|---|---|---|
| `hostsNotConnectedLongTime` | `Counter32` | .1.3.6.1.4.1.23668.1093.1.5.5 | Número de dispositivos que no se han conectado al Servidor de administración durante mucho tiempo. La cantidad de tiempo considerada larga se especifica en `notConnectedLongTime`. |
| `hostsControlLost` | `Counter32` | .1.3.6.1.4.1.23668.1093.1.5.6 | Número de dispositivos que no están bajo el control del Servidor de administración. |
| `eventsStatus` | `INTEGER { ok(0), warning(1), critical(2) }` | .1.3.6.1.4.1.23668.1093.1.6.1 | Subsistema de estado de eventos. Uno de los siguientes:<br>• **Advertencia**. Uno de los siguientes:<br>Los dispositivos del grupo de Servidores de administración no han buscado actualizaciones de Windows durante mucho tiempo.<br>Hay dispositivos con problemas de estado.<br>• **Crítico**. Uno de los siguientes:<br>Se ha producido una ocurrencia de importancia "crítica" en al menos un dispositivo.<br>Se ha producido un "Error" en al menos un dispositivo.<br>Se ha producido una ocurrencia de tarea incompleta en al menos un dispositivo.<br>Los dispositivos del grupo de Servidores de administración no han buscado actualizaciones de Windows durante mucho tiempo.<br>Hay dispositivos con problemas de estado.<br>• **Entendido**. Ninguna de las anteriores. |
| `criticalEventOccured` | `INTEGER { off(0), on(1) }` | .1.3.6.1.4.1.23668.1093.1.6.2.1 | El motivo `eventsStatus` muestra que hay algunos eventos críticos en el Servidor de administración. Puede obtener el número de esas ocurrencias a través de `criticalEventsCount`.<br>El valor es igual a 1 si hay al menos un evento crítico en algún dispositivo y 0 en caso contrario. |
| `criticalEventsCount` | `Counter32` | .1.3.6.1.4.1.23668.1093.1.6.3 | Número de eventos críticos en el Servidor de administración. |

# Resolución de problemas

Esta sección enumera las soluciones para algunos problemas típicos que puede encontrar al utilizar el servicio SNMP.

## La aplicación de terceros no se puede conectar al servicio SNMP

Asegúrese de que el servicio SNMP esté instalado y configurado como se describe en la sección Configuración del servicio SNMP para usar con Kaspersky Security Center.

## El servicio SNMP está funcionando, pero la aplicación de terceros no puede obtener ningún valor.

Permita el seguimiento del agente SNMP y asegúrese de que se cree un archivo no vacío. Esto significa que el agente SNMP está registrado y funciona correctamente. Después de esto, permita las conexiones desde el servicio SNMP en la configuración del servicio lateral. Si un servicio secundario opera en el mismo host que el agente SNMP, la lista de direcciones IP debe contener la dirección IP de ese host o el `loopback 127.0.0.1`.

El servicio SNMP que se comunica con los agentes debe ejecutarse en Windows. Puede especificar las rutas a los agentes SNMP en el Registro de Windows a través de regedit.

- Para Windows 10, haga lo siguiente:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents
- Para Windows Vista y Windows Server 2008, haga lo siguiente:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SNMP\Parameters\ExtensionAgents

También puede permitir el seguimiento de agentes SNMP a través de regedit.

- Para sistemas de 32 bits:
  HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug
- Para sistemas de 64 bits:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Deb
  "TraceLevel"=dword:00000004
  "TraceDir"="C:\\"

### Los valores no coinciden con los estados de la Consola de administración

Para reducir la carga en el Servidor de administración, se implementa el almacenamiento en caché de valores para el agente SNMP. La latencia entre la caché que se actualiza y los valores que se cambian en el Servidor de administración puede causar discrepancias entre los valores devueltos por el agente SNMP y los reales. Cuando trabaje con aplicaciones de terceros, debe tener en cuenta esa posible latencia.

# Trabajo en un entorno de nube

Esta sección proporciona información que le servirá para desplegar y mantener Kaspersky Security Center en un entorno de nube, como Amazon Web Services, Microsoft Azure o Google Cloud.

Las direcciones de las páginas web que se mencionan en este documento eran válidas al momento de la publicación de Kaspersky Security Center.

Es posible que la funcionalidad de las actualizaciones (incluida la provisión de actualizaciones de firmas antivirus y actualizaciones de base de código) y la funcionalidad de KSN no estén disponibles en el software en los EE. UU.

# Acerca del trabajo en un entorno de nube

Kaspersky Security Center 15.1 no solo funciona con dispositivos locales, sino que también proporciona características especiales para trabajar en un entorno de nube. Kaspersky Security Center funciona con las siguientes máquinas virtuales:

- Instancias de Amazon EC2 (en adelante, también denominadas *instancias*). Una instancia de Amazon EC2 es una máquina virtual que se crea sobre la base de la plataforma de servicios web de Amazon (AWS). Kaspersky Security Center utiliza AWS *API* (interfaz de programación de aplicaciones).
- Máquinas virtuales de Microsoft Azure. Kaspersky Security Center usa la API de Azure.
- Instancias de máquinas virtuales de Google Cloud. Kaspersky Security Center utiliza la API de Google.

Puede instalar Kaspersky Security Center en una instancia o en una máquina virtual para administrar la protección de dispositivos en un entorno de nube y usar las características especiales de Kaspersky Security Center para trabajar en un entorno de nube. Estas funciones incluyen:

- La utilización de herramientas API para sondear dispositivos en un entorno de nube
- Uso de herramientas API para instalar el Agente de red y aplicaciones de seguridad en dispositivos en un entorno de nube
- La búsqueda de dispositivos según si pertenecen a un segmento de la nube específico

También puede usar una instancia o una máquina virtual en la que se haya instalado un Servidor de administración de Kaspersky Security Center para proteger los dispositivos locales (por ejemplo, si un servidor en la nube resulta ser más fácil de mantener que uno físico). Si este es el caso, trabajará con el Servidor de administración de la misma manera que lo haría si el Servidor de administración se instalara en un dispositivo local.

Cuando Kaspersky Security Center se instala desde una imagen de máquina de Amazon (AMI) pagada (en AWS) o una SKU facturada mensualmente basada en el uso (en Azure), la característica Administración de vulnerabilidades y parches (incluida la integración con los sistemas SIEM) se activa automáticamente; la característica Administración de dispositivos móviles no se puede activar.

El Servidor de administración se instala junto con la Consola de administración. Kaspersky Security for Windows Server también se instala automáticamente en el dispositivo en el que está instalado el Servidor de administración.

Puede configurar Kaspersky Security Center con el Asistente de configuración del entorno de nube, teniendo en cuenta las particularidades de trabajar en un entorno de nube.

# Escenario: Despliegue en un entorno de nube

En esta sección, se describe el procedimiento para desplegar y utilizar Kaspersky Security Center en un entorno de nube como Amazon Web Services, Microsoft Azure y Google Cloud.

Al concluir este escenario, el Servidor de administración de Kaspersky Security Center y la Consola de administración estarán en funcionamiento con la configuración predeterminada. La protección antivirus administrada por Kaspersky Security Center se despliega en las instancias de Amazon EC2 o en las máquinas virtuales de Microsoft Azure seleccionadas. Luego, puede ajustar la configuración de Kaspersky Security Center, crear una estructura compleja de grupos de administración y crear diferentes directivas y tareas para grupos.

El despliegue de Kaspersky Security Center para trabajar en entornos de nube consta de las siguientes partes:

1. Trabajo de preparación.
2. Despliegue del Servidor de administración.
3. Instalación de las aplicaciones antivirus de Kaspersky en los dispositivos virtuales que se necesite proteger.
4. Configuración de la descarga de actualizaciones.
5. Configurar los parámetros para administrar informes sobre el estado de protección de dispositivos.

El Asistente de configuración del entorno de nube está diseñado para realizar la configuración inicial. Se inicia automáticamente la primera vez que Kaspersky Security Center se despliega desde una imagen lista para usar. Puede iniciar este asistente de manera manual en cualquier momento. También puede llevar a cabo manualmente todas las acciones que realiza.

Recomendamos que separe al menos una hora para desplegar el Servidor de administración de Kaspersky Security Center en el entorno de nube y al menos un día de trabajo para desplegar la protección en el entorno de nube.

El proceso para desplegar Kaspersky Security Center en un entorno de nube se divide en etapas:

1. **Planificación de la configuración de segmentos de la nube**

   Aprenda sobre el funcionamiento de Kaspersky Security Center en un entorno de nube. Evalúe dónde instalará el Servidor de administración (dentro o fuera del entorno de nube) y determine cuántos segmentos de la nube necesitará proteger. Si planea desplegar el Servidor de administración fuera del entorno de nube o si planea proteger más de 5000 dispositivos, necesitará instalar manualmente el Servidor de administración.

   Para trabajar con Google Cloud, solo puede instalar el Servidor de administración manualmente.

2. **Planificando los recursos**

   Asegúrese de tener todo lo necesario para el despliegue.

3. **Suscripción a Kaspersky Security Center como imagen lista para usar**

   Seleccione una de las AMI listas para usar en el Mercado de AWS, o seleccione una SKU facturada mensualmente basada en uso en Azure Marketplace, pague según las reglas del mercado si es necesario (o use el modelo BYOL), y luego use la imagen para desplegar una instancia de Amazon EC2 o una máquina virtual de Microsoft Azure con Kaspersky Security Center instalado.

   Esta etapa solamente es necesaria si planea desplegar el Servidor de administración en una instancia o máquina virtual dentro de un entorno de nube y piensa proteger un máximo de 5000 dispositivos. Fuera de estos casos, omita esta etapa y, en su lugar, instale el Servidor de administración, la Consola de administración y el DBMS manualmente.

   Este paso no está disponible para Google Cloud.

4. **Determinación de la ubicación del DBMS**

   Decida dónde estará su DBMS.

   Si planea utilizar una base de datos fuera del entorno de nube, asegúrese de tener una base de datos que funcione.

   Si planea utilizar Amazon Relational Database Service (RDS), cree una base de datos con RDS en el entorno de nube de AWS.

   Si planea utilizar Microsoft Azure SQL como DBMS, cree una base de datos con el servicio Azure Database en el entorno de nube de Microsoft Azure.

Si planea utilizar Google MySQL, cree una base de datos en Google Cloud (visite https://cloud.google.com/sql/docs/mysql para más detalles
**https://cloud.google.com/sql/docs/mysql**
**).**

5. **Instalación manual del Servidor de administración y la Consola de administración (basada en Microsoft Management Console y/o en la consola web) en dispositivos seleccionados**

   Siguiendo las instrucciones del escenario de instalación principal de Kaspersky Security Center, instale el Servidor de administración, la Consola de administración y el DBMS en los dispositivos seleccionados.

   Esta etapa solo es necesaria cuando el Servidor de administración va a estar ubicado fuera del entorno de nube o si piensa proteger más de 5000 dispositivos. Si se da alguna de estas condiciones, verifique que se cumplan los requisitos de hardware para el Servidor de administración. Fuera de estos casos, esta etapa puede obviarse: bastará con que cuente con una suscripción a Kaspersky Security Center como imagen lista para usar de AWS Marketplace, Azure Marketplace o Google Cloud.

6. **Verifique que el Servidor de administración tenga permisos para operar con las API de la nube**

   En AWS, vaya a la Consola de administración de AWS y cree una función de IAM o una cuenta de usuario de IAM. La función de IAM (o la cuenta de usuario de IAM) que cree permitirá que Kaspersky Security Center trabaje con la API de AWS y que sea posible sondear los segmentos de la nube y desplegar la protección.

   En Azure, cree una suscripción, un id. de la aplicación y la contraseña correspondiente.
   Kaspersky Security Center usará estas credenciales para operar con la API de Azure, sondear los segmentos de nube y desplegar la protección.

   En Google Cloud, registre un proyecto, obtenga su ID de proyecto y una clave privada. Kaspersky Security Center utiliza estas credenciales para sondear segmentos de la nube utilizando la API de Google.

7. **Creación de una función de IAM para instancias protegidas (solo para AWS)**

   En la Consola de administración de AWS, cree una función de IAM que defina el conjunto de permisos para enviar solicitudes a AWS. Este rol recientemente creado se asignará posteriormente a nuevas instancias. La función de IAM se requiere para usar Kaspersky Security Center para instalar aplicaciones en instancias.

8. **Preparación de una base de datos utilizando el servicio Amazon Relational Database Service o Microsoft Azure SQL**

   Si planea utilizar el servicio Amazon RDS, cree una instancia de base de datos de Amazon RDS y un bucket de S3 para almacenar la copia de seguridad de la base de datos. Omita esta etapa si la base de datos estará ubicada en la misma instancia de EC2 que el Servidor de administración o en cualquier otro sitio.

   Si planea usar Microsoft Azure SQL, cree una cuenta de almacenamiento y una base de datos en Microsoft Azure.

   Si planea utilizar Google MySQL, configure su base de datos en Google Cloud (visite https://cloud.google.com/sql/docs/mysql para más detalles).

9. **Licencia de Kaspersky Security Center para trabajar en el entorno de nube**

   Asegúrese de tener la licencia necesaria para usar Kaspersky Security Center en el entorno de nube. Proporcione el código de activación o el archivo de clave necesarios a fin de que la aplicación agregue ese código o archivo al repositorio de licencias. Esta etapa se puede completar durante la configuración del entorno de nube.

   Esta etapa no se puede omitir si Kaspersky Security Center se ha instalado a partir de una AMI lista para usar sin costo basada en el modelo "BYOL", o si Kaspersky Security Center se ha instalado manualmente sin usar una AMI. En ambos casos, necesitará una licencia para Kaspersky Security for Virtualization, o una licencia para seguridad de la nube del híbrido de Kaspersky, para activar Kaspersky Security Center.

   Si utiliza Kaspersky Security Center instalado con una imagen lista para usar, esta etapa no es necesaria y no se mostrará la ventana correspondiente al Asistente de configuración del entorno de nube.

10. **Autorícese en el entorno de nube**

Proporcione a Kaspersky Security Center sus credenciales de AWS, Azure o Google Cloud para que Kaspersky Security Center pueda operar con los permisos necesarios. Esta fase se puede completar durante la autorización en el entorno de nube.

11. **Sondeo de un segmento de la nube para que el Servidor de administración reciba la información sobre dispositivos en el segmento de la nube**

    Inicie el sondeo de segmentos de nube. En el entorno de AWS, Kaspersky Security Center recibirá las direcciones y los nombres de todas las instancias a las que se puede acceder en función de los permisos de la función de IAM o del usuario de IAM. En el entorno de Microsoft Azure, Kaspersky Security Center recibirá las direcciones y los nombres de todas las máquinas virtuales a las que se puede acceder según los permisos de la función de lector.

    Luego puede usar Kaspersky Security Center para instalar aplicaciones y software de Kaspersky de otros proveedores en las instancias o máquinas virtuales detectadas.

    Kaspersky Security Center inicia regularmente un sondeo, lo que significa que las nuevas instancias o máquinas virtuales se detectan automáticamente.

12. **La combinación de todos los dispositivos de la red en el grupo de administración Cloud**

    Mueva las instancias o máquinas virtuales descubiertas al grupo de administración **Dispositivos administrados\Cloud** para que se las pueda administrar en forma centralizada. Si desea asignar distintos dispositivos a distintos subgrupos (basándose, por ejemplo, en el sistema operativo instalado), puede crear esos grupos de administración dentro del grupo **Dispositivos administrados\Cloud**. Puede hacer que los dispositivos detectados durante los sondeos periódicos sean movidos automáticamente al grupo **Dispositivos administrados\Cloud**.

13. **Usar el Agente de red para conectar dispositivos en red al Servidor de administración**

    Instale el Agente de red en los dispositivos disponibles en el entorno de nube. El Agente de red es el componente de Kaspersky Security Center que proporciona comunicación entre los dispositivos y el Servidor de administración. La configuración de Agente de red se ajusta automáticamente de forma predeterminada.

    Puede instalar el Agente de red en cada dispositivo localmente. También puede instalar el Agente de red en los dispositivos de manera remota, a través de Kaspersky Security Center. Como alternativa, también puede saltear esta etapa e instalar el Agente de red junto con las últimas versiones de las aplicaciones de seguridad.

14. **Instalación de las versiones más recientes de aplicaciones de seguridad en dispositivos en red**

    Seleccione los dispositivos en los cuales desee instalar aplicaciones de seguridad y luego instale en ellos las últimas versiones de esas aplicaciones. Puede realizar la instalación de forma remota utilizando Kaspersky Security Center en el Servidor de administración o localmente.

    Es posible que deba crear paquetes de instalación para estos programas en forma manual.

    Kaspersky Endpoint Security for Linux está pensado para instancias y máquinas virtuales con Linux.

    Kaspersky Security for Windows Server está destinado a instancias y máquinas virtuales que ejecutan Windows.

15. **Configuración de parámetros de actualización**

La tarea **Buscar vulnerabilidades y actualizaciones requeridas** se crea automáticamente cuando empiece a configurar el entorno de la nube. Esta tarea también se puede crear manualmente. Esta tarea encuentra y descarga automáticamente actualizaciones de la aplicación requeridas para la instalación subsiguiente en la red dispositivos usando herramientas de Kaspersky Security Center.

Se recomienda completar la siguiente etapa una vez finalizada la configuración del entorno de nube:

1. **Configure los ajustes de administración de informes**

    Puede ver informes en la pestaña **Supervisión** del espacio de trabajo del nodo **Servidor de administración**. También puede recibir informes por correo electrónico. Los informes de la pestaña **Supervisión** están disponibles de forma predeterminada. Para configurar el envío de informes por correo electrónico, introduzca las direcciones de correo electrónico que deban recibir los informes y luego configure el formato de los informes.

### Resultados

Al concluir este escenario, haga lo siguiente para comprobar que la configuración inicial se haya realizado correctamente:

- Verifique si puede conectarse al Servidor de administración a través de la Consola de administración o de Kaspersky Security Center Web Console.
- Verifique si los dispositivos administrados tienen instaladas y en ejecución las versiones más recientes de las aplicaciones de seguridad de Kaspersky.
- Compruebe que Kaspersky Security Center haya creado las directivas y tareas predeterminadas para todos los dispositivos administrados.

## Requisitos previos para desplegar Kaspersky Security Center en un entorno de nube

Antes de comenzar con el despliegue de Kaspersky Security Center en Amazon Web Services o en el entorno de nube de Microsoft Azure, asegúrese de tener lo siguiente:

- Acceso a Internet
- Una de las siguientes cuentas:
  - Cuenta de Amazon Web Services (para trabajar con AWS)
  - Cuenta de Microsoft (para trabajar con Azure)
  - Cuenta de Google (para trabajar con Google Cloud)
- Uno de los siguientes:
  - Licencia para Kaspersky Security for Virtualization
  - Licencia para Kaspersky Hybrid Cloud Security
  - Fondos para comprar la licencia correspondiente para Kaspersky Security for Virtualization o Kaspersky Hybrid Cloud Security
  - Fondos para pagar por una imagen lista para usar en Azure Marketplace
- Guías para las últimas versiones de Kaspersky Endpoint Security para Linux y Kaspersky Security for Windows Server

# Requisitos de hardware para el Servidor de administración en un entorno de nube

Para despliegues en entornos de nube, los requisitos que se exigen para el Servidor de administración y el servidor de bases de datos son los mismos que se exigen para un Servidor de administración físico (los requisitos variarán en función de la cantidad de dispositivos que busque administrar). Encontrará más detalles en la documentación del entorno de nube.

# Opciones de licencia en un entorno de nube

Trabajar en el entorno de nube está fuera de la funcionalidad básica de Kaspersky Security Center, por tanto, requiere una licencia específica.

Hay dos opciones de licencia de Kaspersky Security Center disponibles para trabajar en un entorno de nube:

- AMI pagada (en Amazon Web Services) o SKU facturado en función del uso (en Microsoft Azure).

  Esto otorga una licencia para Kaspersky Security Center, así como licencias para Kaspersky Endpoint Security para Linux y Kaspersky Security for Windows Server. Debe pagar de acuerdo con las reglas del entorno de nube que utilice.

  Este modelo no le permite tener más de 200 dispositivos cliente para un Servidor de administración.

- Una imagen de uso gratuito y lista para usar con una licencia de propietario, según el modelo de su propia licencia (BYOL).

  Para las licencias de Kaspersky Security Center en AWS o Azure, debe tener una licencia para una de las siguientes aplicaciones:

  - Kaspersky Security for Virtualization
  - Kaspersky Hybrid Cloud Security

  El modelo BYOL le permite tener hasta 100 000 dispositivos cliente para un Servidor de administración. Este modelo también le permite administrar dispositivos fuera del entorno de nube de AWS, Azure o Google.

  Puede elegir el modelo BYOL en cualquiera los siguientes casos:

  - Ya posee una licencia válida de Kaspersky Security for Virtualization.
  - Ya posee una licencia válida para seguridad de la nube del híbrido de Kaspersky.
  - Está dispuesto a comprar una licencia inmediatamente antes comenzar con el despliegue de Kaspersky Security Center.

  En la etapa de la instalación inicial, Kaspersky Security Center le solicitará un código de activación o un archivo de clave.

  Si elige BYOL, no tendrá que pagar Kaspersky Security Center a través de Azure Marketplace o Plataforma AWS.

En ambos casos, la Administración de vulnerabilidades y parches se activa automáticamente, y la Administración de dispositivos móviles no se puede activar.

Si se produce un error al intentar activar la función Soporte del entorno de nube con la licencia de Kaspersky Hybrid Cloud Security, use el archivo de clave.

Al suscribirse a Kaspersky Security Center, obtiene una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o una máquina virtual de Microsoft Azure con el Servidor de administración de Kaspersky Security Center . Los paquetes de instalación para Kaspersky Security for Windows Server y Kaspersky Endpoint Security para Linux están disponibles en el Servidor de administración. Puede instalar estas aplicaciones en dispositivos en el entorno de nube. No tiene que licenciar estas aplicaciones.

Si el Servidor de administración no puede ver un dispositivo administrado durante más de una semana, la aplicación (Kaspersky Security for Windows Server o Kaspersky Endpoint Security para Linux) cambiará al modo de funcionalidad limitada en el dispositivo. Para volver a activar la aplicación, debe hacer que el Servidor de administración vuelva a ver el dispositivo en el que está instalada la aplicación.

# Opciones de base de datos para trabajar en un entorno de nube

Debe tener una base de datos para trabajar con Kaspersky Security Center. Cuando el despliegue de Kaspersky Security Center se lleva a cabo en AWS, en Microsoft Azure o en Google Cloud, existen tres opciones:

- Crear una base de datos local en el mismo dispositivo con el Servidor de administración. Kaspersky Security Center viene con una base de datos SQL Server Express que puede admitir hasta 5000 dispositivos administrados. Elija esta opción si SQL Server Express Edition es suficiente para sus necesidades.
- Crear una base de datos con el Servicio de bases de datos relacionales (RDS) en el entorno de nube de AWS o con el Servicio de base de datos de Azure en el entorno de nube de Microsoft Azure. Elija esta opción si desea un DBMS que no sea SQL Express. Sus datos se transferirán dentro del entorno de nube, donde permanecerán y no tendrá ningún gasto adicional. Si ya trabaja con Kaspersky Security Center en las instalaciones y tiene algunos datos en su base de datos, puede transferir sus datos a la nueva base de datos.

  Para trabajar en Google Cloud Platform, solo puede usar Cloud SQL para MySQL.
- Utilice un servidor de la base de datos existente. Elija esta opción si ya tiene un servidor de la base de datos y desea usarlo para Kaspersky Security Center. Si este servidor está fuera del entorno de nube, sus datos se transferirán a Internet, lo que podría causar gastos adicionales.

El procedimiento para desplegar Kaspersky Security Center en el entorno de nube tiene un paso especial para crear (elegir) una base de datos.

# Trabajar en el entorno de nube de Amazon Web Services

En esta sección, aprenderá a prepararse para trabajar con Kaspersky Security Center en Amazon Web Services.

Las direcciones de las páginas web que se mencionan en este documento eran válidas al momento de la publicación de Kaspersky Security Center.

# Acerca del trabajo con el entorno de nube de Amazon Web Services

Puede comprar Kaspersky Security Center en la AWS Marketplace como un AMI (imagen de máquina de Amazon), que es una imagen lista de una máquina virtual preconfigurada. Puede suscribirse a una AMI pagada o BYOL AMI y, según esa imagen, crear una instancia de Amazon EC2 con el Servidor de administración de Kaspersky Security Center instalado.

Para funcionar con la plataforma AWS y, en particular, comprar aplicaciones en la AWS Marketplace y crear instancias, necesitará una cuenta de Amazon Web Services. Puede crear una cuenta sin costo en https://aws.amazon.com. Si ya tiene una cuenta de Amazon, puede usarla.

Si se suscribió a una AMI disponible en AWS Marketplace, recibirá una instancia con su Kaspersky Security Center listo para usar. No tiene que instalar la aplicación usted mismo. En este caso, Servidor de administración de Kaspersky Security Center se instala en la instancia sin su participación. Después de la instalación, puede iniciar la Consola de administración y conectarse al Servidor de administración para comenzar a trabajar con Kaspersky Security Center.

Encontrará información sobre las imágenes AMI y sobre el funcionamiento de la plataforma AWS en la página de ayuda de AWS Marketplace. Si precisa más información sobre el uso de la plataforma AWS, el uso de las instancias y otros conceptos, consulte la documentación de Amazon Web Services.

Las direcciones de las páginas web que se mencionan en este documento eran válidas al momento de la publicación de Kaspersky Security Center.

# Creación de funciones de IAM y cuentas de usuario de IAM para instancias de Amazon EC2

Esta sección describe las acciones que se deben realizar para garantizar el funcionamiento correcto del Servidor de administración. Estas acciones incluyen el trabajo con las funciones y las cuentas de usuario de AWS Identity and Access Management (IAM). También se describen las acciones que deberá realizar en los dispositivos cliente para instalar en ellos el Agente de red y, posteriormente, Kaspersky Security for Windows Server y Kaspersky Endpoint Security for Linux.

## Comprobar que el Servidor de administración de Kaspersky Security Center tenga los permisos para trabajar con AWS

Los estándares para operar en el entorno de nube de Amazon Web Services (AWS) prescriben que se asigne una función de IAM especial a la instancia del Servidor de administración para trabajar con los servicios de AWS. Una función de IAM es una entidad de IAM que define el conjunto de permisos para la ejecución de solicitudes a servicios de AWS. La función de IAM proporciona los permisos para el sondeo de segmentos de la nube y la instalación de aplicaciones en instancias.

Después de crear una función de IAM y asignarla al Servidor de administración, podrá desplegar la protección de las instancias mediante el uso de esta función, sin proporcionar información adicional a Kaspersky Security Center.

Sin embargo, puede ser aconsejable no crear una función de IAM para el Servidor de administración en los siguientes casos:

- Los dispositivos cuya protección planea administrar son instancias EC2 dentro del entorno de nube de Amazon Web Services, pero el Servidor de administración está fuera de este entorno.

- Planea administrar la protección de instancias no solo dentro de su segmento de la nube sino también dentro de otros segmentos de nube que se crearon con una cuenta diferente en AWS. En este caso, necesitará una función de IAM solo para la protección de su segmento de la nube. No será necesaria una función de IAM para proteger otro segmento de la nube.

En estos casos, en lugar de crear una función de IAM, deberá crear una *cuenta de usuario de IAM* que Kaspersky Security Center utilizará para trabajar con los servicios de AWS. Antes de comenzar a trabajar con el Servidor de administración, cree una cuenta de usuario de IAM con una *clave de acceso de AWS IAM* (en lo sucesivo, también se usará el término *clave de acceso de IAM*).

La creación de una función de IAM o de una cuenta de usuario de IAM requiere la Consola de administración de AWS. Para trabajar con la Consola de administración de AWS, necesitará el nombre de usuario y la contraseña de una cuenta de AWS.

## Crear una función de IAM para el Servidor de administración

Antes de instalar el Servidor de administración, en la Consola de administración de AWS cree una función de IAM con los permisos necesarios para la instalación de aplicaciones en instancias. Para obtener más información, consulte las secciones de Ayuda de AWS acerca de las funciones de IAM.

*Para crear una función de IAM para el Servidor de administración:*

1. Abra la Consola de administración de AWS e inicie sesión en su cuenta de AWS.

2. En la sección **Roles**, cree un rol con los siguientes permisos:

   - **AmazonEC2ReadOnlyAccess**, si planea ejecutar solo el sondeo de segmento de la nube y no planea instalar aplicaciones en instancias EC2 con API de AWS.

   - **AmazonEC2ReadOnlyAccess** y **AmazonSSMFullAccess**, si planea ejecutar el sondeo de segmento de la nube e instalar aplicaciones en instancias de EC2 con API de AWS. En este caso, también deberá asignar una función de IAM con el permiso AmazonEC2RoleforSSM a las instancias de EC2 protegidas.

Deberá asignar esta función a la instancia de EC2 que usará como Servidor de administración.

El rol recién creado está disponible para todas las aplicaciones en el Servidor de administración. Por lo tanto, cualquier aplicación que se ejecute en el Servidor de administración tiene la capacidad de sondear segmentos en la nube o instalar aplicaciones en instancias de EC2 dentro de un segmento de la nube.

Las direcciones de las páginas web que se mencionan en este documento eran válidas al momento de la publicación de Kaspersky Security Center.

## Creación de una cuenta de usuario de IAM para trabajar con Kaspersky Security Center

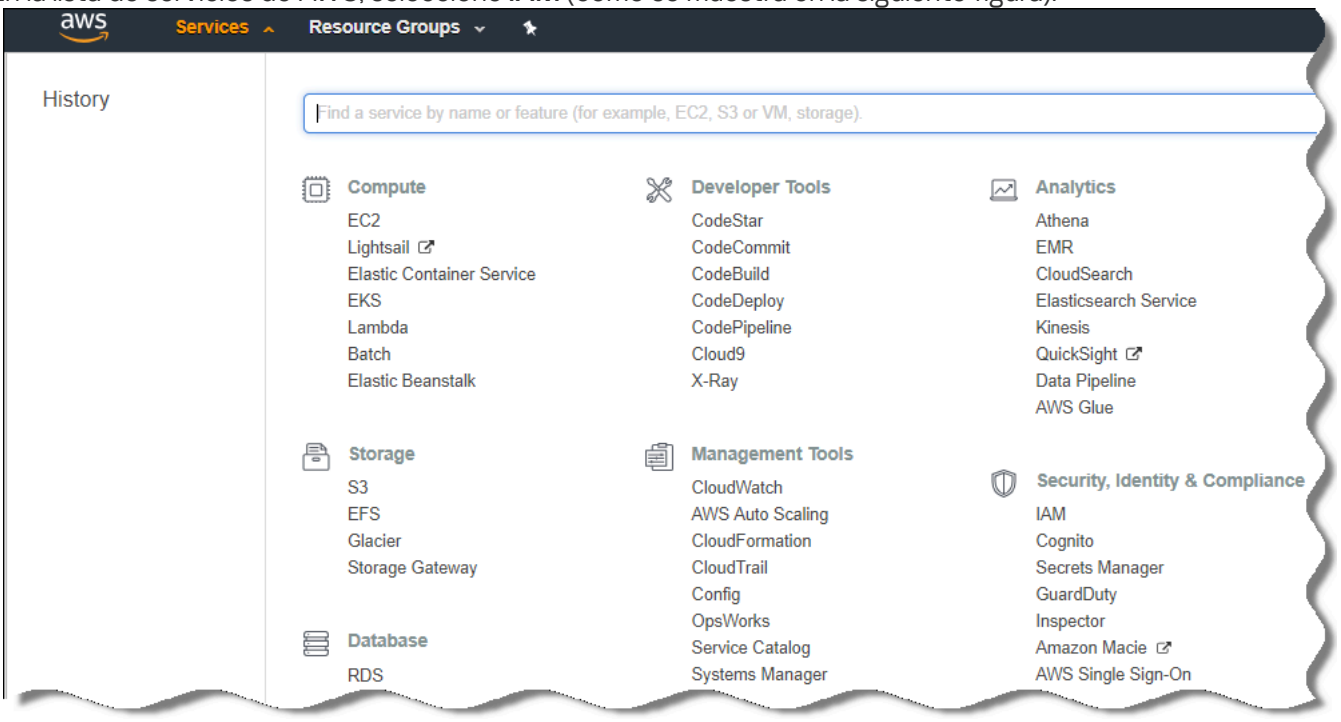
Se necesita una cuenta de usuario de IAM para trabajar con Kaspersky Security Center si al Servidor de administración no se le ha asignado una función de IAM con permisos para efectuar el descubrimiento de dispositivos e instalaciones de aplicaciones en las instancias. La misma cuenta, o una cuenta diferente, también se requiere para hacer una copia de seguridad de la tarea de datos del Servidor de administración si usa un bucket de S3. Puede crear una cuenta de usuario de IAM con todos los permisos necesarios o, si lo prefiere, puede crear dos cuentas de usuario separadas.

Se creará automáticamente para el usuario de IAM una *clave de acceso de IAM*, que usted deberá proporcionar a Kaspersky Security Center durante la configuración inicial. La clave de acceso de IAM consiste en un id. de clave de acceso y una clave secreta. Para obtener más información sobre el servicio de IAM, consulte las siguientes páginas de referencia de AWS:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html.
- http://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

*Para crear una cuenta de usuario de IAM con los permisos necesarios, haga lo siguiente:*

1. Abra la Consola de administración de AWS e inicie sesión con su cuenta.
2. En la lista de servicios de AWS, seleccione **IAM** (como se muestra en la siguiente figura).




Lista de servicios en la Consola de administración de AWS

Se abrirá una ventana con una lista de nombres de usuario y un menú para trabajar con la herramienta.

3. Navegue por las áreas de la consola relacionadas con las cuentas de usuario y agregue uno o más nombres de usuario nuevos.

4. Especifique las siguientes propiedades de AWS para cada usuario agregado:

   - Tipo de acceso: **Programmatic Access**.
   - Límite de permisos no establecido.
   - Permisos:
     - **ReadOnlyAccess**, si planea realizar únicamente sondeos en los segmentos de la nube y no tiene pensado instalar aplicaciones en las instancias de EC2 utilizando la API de AWS.
     - **ReadOnlyAccess** y **AmazonSSMFullAccess**, si planea realizar sondeos en los segmentos de la nube y también tiene pensado instalar aplicaciones en las instancias de EC2 utilizando la API de AWS. En este caso, deberá asignar una función de IAM con el permiso AmazonEC2RoleforSSM a las instancias de EC2 protegidas.

   Después de añadir los permisos, revíselos para asegurarse de que sean correctos. Si comete un error al hacer una selección, regrese a la pantalla anterior y vuelva a realizar la selección.

5. Después de crear la cuenta de usuario, aparecerá una tabla con la clave de acceso de IAM correspondiente al nuevo usuario de IAM. El id. de la clave de acceso estará en la columna **Access key ID**. La clave secreta se mostrará como una secuencia de asteriscos en la columna **Secret access key**. Para ver la clave secreta, haga clic en **Show**.

   La cuenta que acaba de crear aparecerá en la lista de cuentas de usuario de IAM correspondiente a su cuenta de AWS.

Cuando Kaspersky Security Center se instala en un segmento de la nube, es necesario especificar que se está utilizando una cuenta de usuario de IAM y proporcionarle el id. de clave de acceso y la clave de acceso secreta a Kaspersky Security Center.

Las direcciones de las páginas web que se mencionan en este documento eran válidas al momento de la publicación de Kaspersky Security Center.

## Creación de una función de IAM para la instalación de aplicaciones en instancias de Amazon EC2

Antes de comenzar a desplegar la protección a las instancias de EC2 usando Kaspersky Security Center, cree en la Consola de administración de AWS una función de IAM con los permisos requeridos para la instalación de aplicaciones en instancias. Para obtener más información, consulte las secciones de Ayuda de AWS Ayuda de AWS acerca de las funciones de IAM

La función de IAM es necesaria porque deberá asignarla a todas las instancias de EC2 en las que planee instalar aplicaciones de seguridad usando Kaspersky Security Center. Si no asigna a una instancia la función de IAM con los permisos necesarios, la instalación de aplicaciones en esta instancia usando herramientas de API de AWS causará un error.

Para trabajar con la Consola de administración de AWS, necesitará el nombre de usuario y la contraseña de una cuenta de AWS.

*Para crear una función de IAM para instalar aplicaciones en instancias:*

1. Abra la Consola de administración de AWS e inicie sesión en su cuenta de AWS.
2. En el menú a la izquierda, seleccione **Roles**.
3. Haga clic en el botón **Create Role**.
4. En la lista de servicios que aparece, seleccione **EC2** y, luego, en la lista **Select Your Use Case**, vuelva a seleccionar **EC2**.
5. Haga clic en el botón **Next: Permissions**.
6. En la lista que se abre, seleccione la casilla al lado de **AmazonEC2RoleforSSM**.
7. Haga clic en el botón **Next: Review**.
8. Ingrese un nombre y una descripción para la función de IAM y haga clic en el botón **Create role**.

   El rol que creó aparece en la lista de roles con el nombre y la descripción que ingresó.

En lo sucesivo, podrá usar la nueva función de IAM para crear las instancias de EC2 que quiera proteger a través de Kaspersky Security Center. También podrá asociar la función con instancias existentes.

> Las direcciones de las páginas web que se mencionan en este documento eran válidas al momento de la publicación de Kaspersky Security Center.

## Trabajar con Amazon RDS

Esta sección describe qué acciones se deben tomar para preparar una base de datos del Servicio de bases de datos relacionales de Amazon (RDS) para Kaspersky Security Center, ubicarla en un grupo de opciones, crear una función de IAM para trabajar con una base de datos de RDS, preparar un bucket de S3 para el almacenamiento y migrar una base de datos existente a RDS.

Amazon RDS es un servicio web que ayuda a los usuarios de AWS a configurar, operar y escalar una base de datos relacional en el entorno de nube de AWS. Si lo desea, puede usar una base de datos de RDS de Amazon para trabajar con Kaspersky Security Center.

Puede trabajar con las siguientes bases de datos:

- Microsoft SQL Server
- SQL Express Edition
- Aurora MySQL 5.7
- Standard MySQL 5.7

## Creación de una instancia de RDS de Amazon

Si desea utilizar Amazon RDS como DBMS, debe crear una instancia de base de datos de Amazon RDS. Esta sección describe cómo seleccionar SQL Express Edition; si desea trabajar con Aurora MySQL o Standard MySQL (versiones 5.7, 8.0), debe seleccionar uno de esos motores.

*Para crear una instancia de base de datos de Amazon RDS:*

1. Abra la Consola de administración de AWS en https://console.aws.amazon.com e inicie sesión en su cuenta.
2. Utilizando la interfaz de AWS, cree una base de datos con la siguiente configuración:
   - Motor: Microsoft SQL Server, SQL Express Edition
   - Versión del motor de DB: SQL Server 2014 12.00.5546.0v1
   - Clase de instancia de BD: db.t2.medium
   - Tipo de almacenamiento: propósito general
   - Almacenamiento asignado: mínimo 50 GiB
   - Grupo de seguridad: el mismo grupo donde se ubicará la instancia de EC2 con el Servidor de administración de Kaspersky Security Center

   Cree un identificador, un nombre de usuario y una contraseña para su instancia de RDS.

   Puede dejar la configuración predeterminada en todos los demás campos. O cambie la configuración predeterminada si desea personalizar su instancia de Amazon RDS. Para obtener ayuda, consulte las páginas de información de AWS.
3. En el último paso, AWS muestra los resultados del proceso. Si desea ver los detalles de su instancia de Amazon RDS, presione **Ver detalles de la instancia de base de datos**. Si desea continuar con la siguiente acción, comience a crear un grupo de opciones para su instancia de Amazon RDS.

La creación de una nueva instancia de Amazon RDS puede llevar varios minutos. Después de crear la instancia, puede usarla para trabajar con los datos de Kaspersky Security Center.

Las direcciones de las páginas web que se mencionan en este documento eran válidas al momento de la publicación de Kaspersky Security Center.

## Creación de un grupo de opciones para la instancia de RDS de Amazon

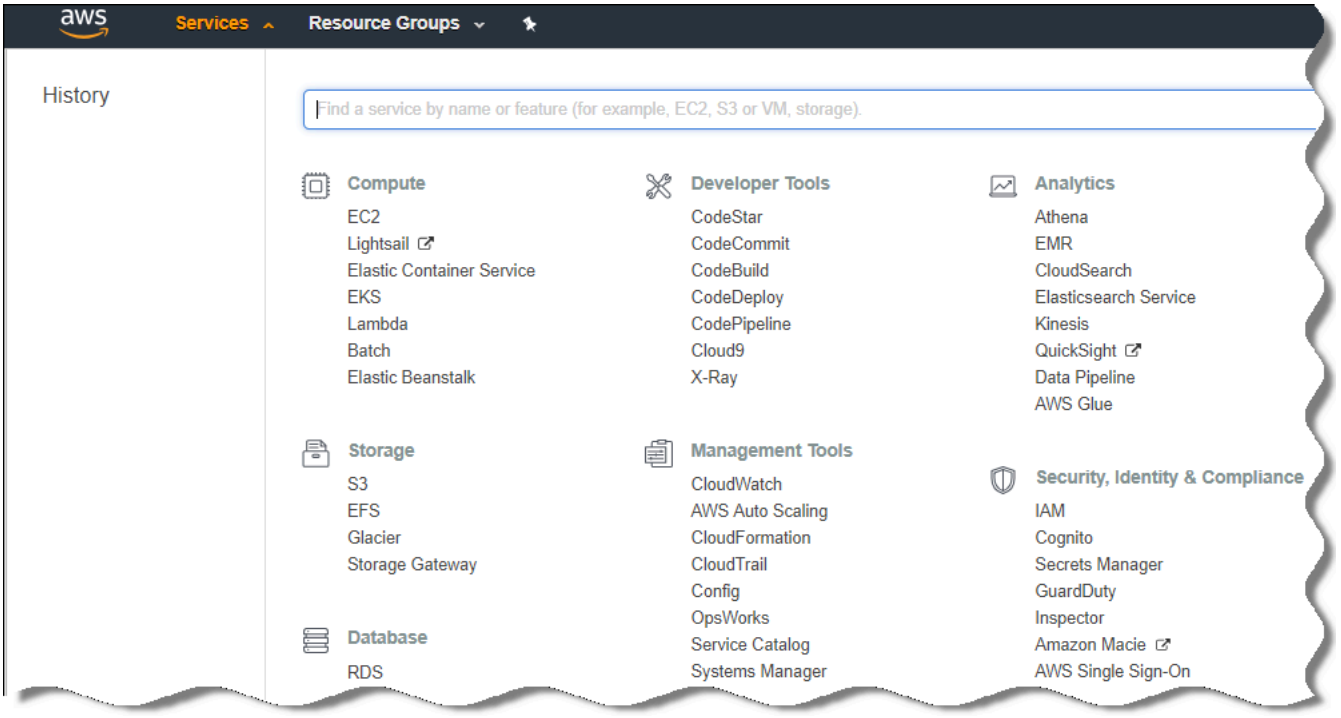
Debe colocar su instancia de Amazon RDS en un grupo de opciones.

*Para crear un grupo de opciones para su instancia de Amazon RDS:*

1. Asegúrese de estar en la Consola de administración de AWS (https://console.aws.amazon.com) y de haber iniciado sesión en su cuenta.

2. En la línea del menú, haga clic en **Services**.

   Aparece la lista de servicios disponibles (ver figura a continuación).




Lista de servicios en la Consola de administración de AWS

3. En la lista, haga clic en **RDS**.

4. En el panel izquierdo, haga clic en **Option groups**.

5. Haga clic en el botón **Create group**.

6. Cree un grupo de opciones con la siguiente configuración, si eligió SQL Server en la etapa de creación de la instancia de Amazon RDS:

   - Motor: SQLserver-ex
   - Versión de motor principal: 12.00

   Si eligió una base de datos SQL diferente en la etapa de creación de la instancia de Amazon RDS, elija un motor correspondiente.

El grupo se crea y se muestra en la lista de grupos.

Después de crear el grupo de opciones, coloque su instancia de Amazon RDS en este grupo de opciones.

Las direcciones de las páginas web que se mencionan en este documento eran válidas al momento de la publicación de Kaspersky Security Center.

## Modificación del grupo de opciones

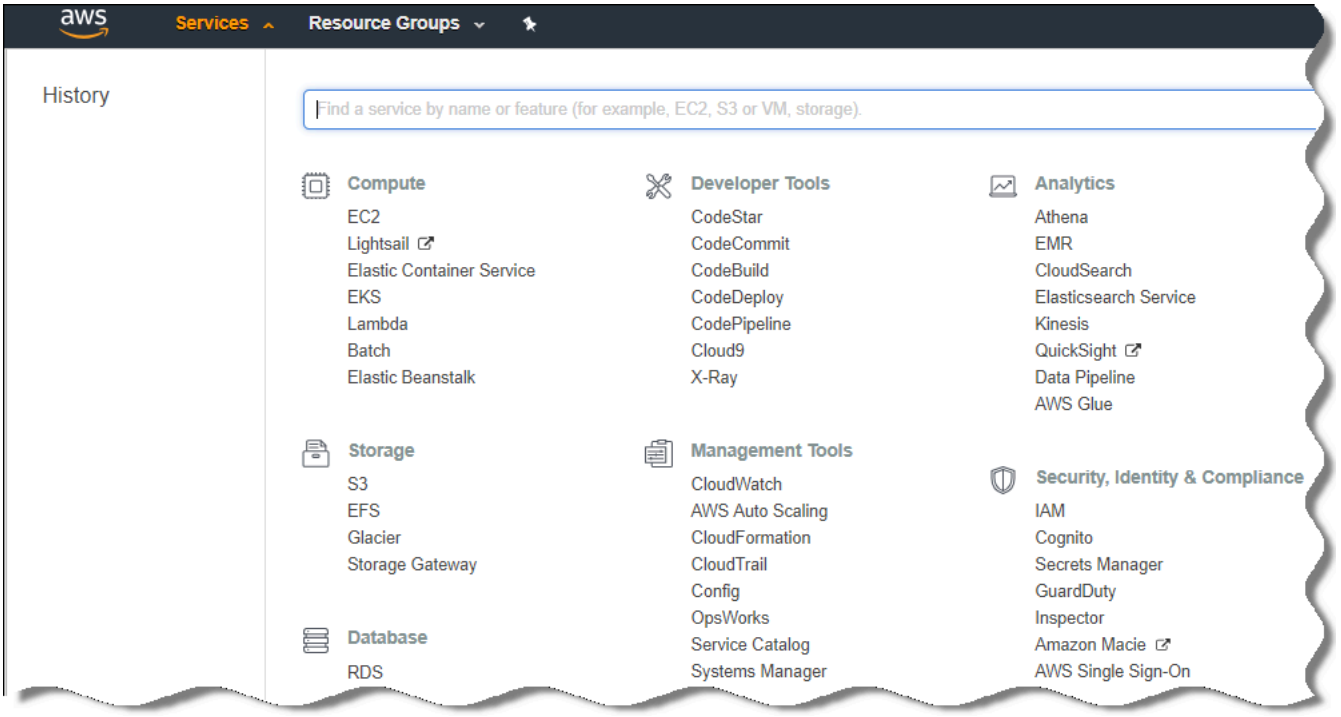
La configuración predeterminada del grupo de opciones en el que colocó la instancia de Amazon RDS no es suficiente para trabajar con la base de datos de Kaspersky Security Center. Debe agregar opciones al grupo de opciones y crear una nueva función de IAM para trabajar con la base de datos.

*Para modificar el grupo de opciones y crear una nueva función de IAM:*

1. Asegúrese de estar en la Consola de administración de AWS (https://console.aws.amazon.com) y de haber iniciado sesión en su cuenta.

2. En la línea del menú, haga clic en **Services**.

   Aparece la lista de servicios disponibles (ver figura a continuación).




Lista de servicios en la Consola de administración de AWS

3. En la lista, seleccione RDS.

4. En el panel izquierdo, haga clic en **Option groups**.

   Se muestra la lista de grupos de opciones.

5. Seleccione el grupo de opciones en el que colocó su instancia de Amazon RDS y haga clic en el botón **Add option**.

   Se abre la ventana **Add option**.

6. En la sección de la función de IAM, seleccione la opción **Add option**/**Yes** e ingrese un nombre para la nueva función de IAM.

   La función se crea con un conjunto predeterminado de permisos. Más adelante, tendrá que cambiar sus permisos.

7. En la sección del bucket de S3, haga uno de los siguientes:

   - Si no ha creado una instancia de bucket de Amazon S3 para la copia de seguridad de datos, seleccione el enlace **Create a new S3 bucket** y cree un nuevo bucket de S3, utilizando la interfaz de AWS.
   - Si ya creó una instancia de cubo de Amazon S3 para la tarea de copia de seguridad de datos del Servidor de administración, seleccione su cubo de S3 en la lista desplegable.

8. Termine de añadir opciones haciendo clic en el botón **Add option** en la parte inferior de la página.

Ha modificado el grupo de opciones y ha creado una nueva función de IAM para trabajar con la base de datos de RDS.

Las direcciones de las páginas web que se mencionan en este documento eran válidas al momento de la publicación de Kaspersky Security Center.

## Modificación de permisos para la función de IAM para la instancia de base de datos de Amazon RDS

Después de agregar opciones al grupo de opciones, debe asignar los permisos necesarios a la función de IAM que creó para trabajar con la instancia de base de datos de Amazon RDS.

*Para asignar los permisos necesarios a la función de IAM que creó para trabajar con la instancia de base de datos de Amazon RDS:*

1. Asegúrese de estar en la Consola de administración de AWS (https://console.aws.amazon.com) y de haber iniciado sesión en su cuenta.
2. En la lista de servicios, seleccione **IAM**.

   Se abrirá una ventana con una lista de nombres de usuario y un menú para trabajar con la herramienta.

3. En el menú, seleccione **Roles**.
4. En la lista de funciones de IAM que se muestran en el espacio de trabajo, seleccione la función que creó al agregar la opción al grupo de opciones.
5. Al usar la interfaz AWS, elimine la directiva **sqlNativeBackup-<fecha>**.
6. Al utilizar la interfaz AWS, adjunte la directiva **AmazonS3FullAccess** a la función.

A la función de IAM se le asignan los permisos necesarios para trabajar con Amazon RDS.

Las direcciones de las páginas web que se mencionan en este documento eran válidas al momento de la publicación de Kaspersky Security Center.

## Preparación del bucket de Amazon S3 para la base de datos

Si planea utilizar la base de datos del Sistema de base de datos relacional de Amazon (Amazon RDS), debe crear una instancia de bucket del Servicio de almacenamiento simple de Amazon (Amazon S3) donde se almacenará la Copia de seguridad regular de la base de datos. Para obtener información sobre Amazon S3 y sobre los buckets de S3, consulte las páginas de ayuda de Amazon

https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/AmazonS3.html
. Para obtener más información sobre cómo crear una instancia de Amazon S3, consulte la página de ayuda de Amazon S3
https://docs.aws.amazon.com/AmazonS3/latest/user-guide/create-bucket.html
.
*Para crear un bucket de Amazon S3:*

1. Asegúrese de que la Consola de administración de AWS esté abierta y de que haya iniciado sesión en su cuenta.
2. En la lista de servicios AWS, seleccione S3.
3. Navegue por la consola para crear un bucket, siguiendo las instrucciones del Asistente.
4. Seleccione la misma región en la que se encuentre (o vaya a encontrarse) su Servidor de administración.
5. Cuando finalice el Asistente, asegúrese de que el nuevo grupo aparezca en la lista de grupos.

   Se crea un nuevo bucket de S3 y aparece en su lista de buckets. Tiene que especificar este bucket al agregar opciones al grupo de opciones. También deberá especificar la dirección de su bucket de S3 en Kaspersky Security Center cuando Kaspersky Security Center cree la tarea de *Copia de seguridad de los datos del Servidor de administración*.

Las direcciones de las páginas web que se mencionan en este documento eran válidas al momento de la publicación de Kaspersky Security Center.

## Migrar la base de datos a Amazonas RDS

Puede migrar su base de datos de Kaspersky Security Center desde un dispositivo local a una instancia de Amazon S3 que admita Amazon RDS. Para hacer esto, necesita un bucket de S3 para una base de datos de RDS y una cuenta de usuario de IAM con el permiso AmazonS3FullAccess para este bucket de S3.

*Para realizar la migración de la base de datos:*

1. Asegúrese de haber creado una instancia de RDS (consulte las páginas de referencia de Amazon RDS para obtener más información).
2. En su Servidor de administración físico (local), ejecute la utilidad de copia de seguridad de Kaspersky para hacer una copia de seguridad de los datos del Servidor de administración.

   Asegúrese de que el nombre del archivo sea backup.zip.

3. Copie el archivo backup.zip a la instancia de EC2 en la que está instalado el Servidor de administración.

   Asegúrese de tener suficiente espacio en el disco en la instancia de EC2 en la que está instalado el Servidor de administración. En el entorno de AWS, puede agregar espacio en disco a su instancia para adaptarse al proceso de migración de la base de datos.

4. En el Servidor de administración de AWS, vuelva a iniciar la utilidad de copia de seguridad de Kaspersky en modo interactivo.

   Se inicia el Asistente de copias de seguridad y restauración.

5. En el paso **Seleccione una acción**, seleccione **Restaurar datos del Servidor de administración** y haga clic en **Siguiente**.

6. En el paso **Opciones de restauración** de la restauración, pulse el botón **Examinar** al lado de la **Carpeta de almacenamiento de copias de seguridad**.

7. En la ventana **Inicie sesión en el almacenamiento en línea** que se abre, complete los siguientes campos y luego haga clic en **Aceptar**:

   - **Nombre del bucket de S3**

     El nombre de su bucket de S3.

   - **Carpeta de la copia de seguridad**

     Especifique la ubicación de la carpeta de almacenamiento que está destinada a la copia de seguridad.

   - **Id. de clave de acceso**

     El id. de clave de acceso de AWS IAM que pertenece al usuario de IAM que tiene los permisos para usar el bucket de S3 (el permiso AmazonS3FullAccess).

   - **Clave secreta**

     La clave secreta de AWS IAM que pertenece al usuario de IAM que tiene los permisos para usar el bucket de S3 (el permiso AmazonS3FullAccess).

8. Seleccione la opción **Migrar desde la copia de seguridad local**. El botón **Examinar estará disponible**.

9. Haga clic en el botón **Examinar** y elija la carpeta del Servidor de administración de AWS en la que haya puesto el archivo backup.zip.

10. Haga clic en **Siguiente** y complete el procedimiento.

Sus datos se restaurarán en la base de datos de RDS utilizando su bucket de S3. Puede usar esta base de datos para seguir trabajando con Kaspersky Security Center en el entorno de AWS.

Las direcciones de las páginas web que se mencionan en este documento eran válidas al momento de la publicación de Kaspersky Security Center.

# Trabajar en el entorno de nube de Microsoft Azure

Esta sección proporciona información que le servirá para desplegar y mantener Kaspersky Security Center en un entorno de nube proporcionado por Microsoft Azure. Encontrará también detalles sobre el despliegue de la protección en las máquinas virtuales de este entorno de nube.

Cuando el despliegue de Kaspersky Security Center se realiza utilizando un SKU facturado en función del uso y en forma mensual, la característica Administración de vulnerabilidades y parches se activa automáticamente; la característica Administración de dispositivos móviles, en cambio, no se puede activar.

## Acerca del uso de Microsoft Azure

Para trabajar con la plataforma Microsoft Azure y, en particular, para comprar aplicaciones en Azure Marketplace y crear máquinas virtuales, necesitará una suscripción de Azure. Antes de instalar el Servidor de administración, cree un id. de aplicación en Azure con los permisos necesarios para la instalación de aplicaciones en máquinas virtuales.

Si compra una imagen de Kaspersky Security Center en Azure Marketplace, puede crear una máquina virtual con su Servidor de administración de Kaspersky Security Center listo para usar. Debe seleccionar la configuración de la máquina virtual pero no tiene que instalar la aplicación usted mismo. Después de la instalación, puede iniciar la Consola de administración y conectarse al Servidor de administración para comenzar a trabajar con Kaspersky Security Center.

También puede usar una máquina virtual de Azure que tenga instalado el Servidor de administración de Kaspersky Security Center para proteger los dispositivos locales (por ejemplo, si un servidor en la nube resulta ser más fácil de inspeccionar y mantener que uno físico). Si este es el caso, trabajará con el Servidor de administración de la misma manera que lo haría si el Servidor de administración se instalara en un dispositivo local. Si no planea usar las herramientas de la API de Azure, no necesitará el Id. de la aplicación en Azure. En este caso, una suscripción de Azure es suficiente.

## Creación de una suscripción, un id. de aplicación y una contraseña

Para trabajar con Kaspersky Security Center en el entorno de Microsoft Azure, necesita una suscripción de Azure, un Id. de la aplicación en Azure y la contraseña de la aplicación en Azure. Si ya tiene una suscripción, puede utilizarla.

Una suscripción de Azure otorga a su titular acceso al Portal de administración de la plataforma Microsoft Azure y a los servicios de Microsoft Azure. El titular puede usar la plataforma Microsoft Azure para administrar servicios como Azure SQL y Azure Storage.

*Para crear una suscripción de Microsoft Azure,*

Vaya a https://learn.microsoft.com/es-mx/azure/cost-management-billing/manage/create-subscription y siga las instrucciones que allí se indican.

Encontrará más detalles sobre la creación de una suscripción en el sitio web de Microsoft website. Obtendrá un id. de suscripción, que luego proporcionará a Kaspersky Security Center junto con el id. de la aplicación y la contraseña.

*Para crear y guardar el id. de aplicación de Azure y su contraseña:*

1. Vaya a https://portal.azure.com y constate que ha iniciado la sesión.
2. Siguiendo las instrucciones de la página de referencia, cree el id. de aplicación.
3. Vaya a la sección **Claves** de la configuración de la aplicación.
4. En la sección **Claves**, complete los campos **Descripción** y **Caducidad**, y deje el campo **Valor** en blanco.
5. Haga clic en **Guardar**.

   Cuando haga clic en **Guardar**, el sistema completará el campo **Valor** automáticamente con una larga secuencia de caracteres. Esta secuencia es la contraseña de la aplicación en Azure (por ejemplo, yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU=). La descripción se muestra a medida que la introduce.
6. Copie la contraseña y guárdela para que luego pueda proporcionar el id. y la contraseña de la aplicación a Kaspersky Security Center.

   Podrá copiar la contraseña solo en el momento en que se la cree. Más adelante, la contraseña ya no se mostrará y no podrá restaurarla.

Las direcciones de las páginas web que se mencionan en este documento eran válidas al momento de la publicación de Kaspersky Security Center.

## Asignación de una función al id. de la aplicación en Azure

Si solo desea detectar máquinas virtuales mediante el descubrimiento de dispositivos, el id. de la aplicación en Azure deberá tener la función de lector. Si no solo desea detectar máquinas virtuales, sino también desplegar la protección en las máquinas virtuales, el id. de la aplicación en Azure debe tener la función de Colaborador de máquina virtual.

Siga las instrucciones del sitio web de Microsoft para asignar una función al id. de la aplicación en Azure.

# Despliegue del Servidor de administración en Microsoft Azure y selección de la base de datos

*Para instalar el Servidor de administración en el entorno de Microsoft Azure:*

1. Inicie sesión en Microsoft Azure utilizando su cuenta.
2. Vaya al portal de Azure.
3. En el recuadro izquierdo, haga clic en el signo más verde.
4. Escriba "Kaspersky Hybrid Cloud Security" en el campo de búsqueda del menú.

   Kaspersky Hybrid Cloud Security es una combinación de Kaspersky Security Center y dos aplicaciones de seguridad para la protección de instancias: Kaspersky Endpoint Security para Linux y Kaspersky Security for Windows Server.
5. En la lista de resultados, seleccione Kaspersky Hybrid Cloud Security o Kaspersky Hybrid Cloud Security (BYOL).

   En la parte derecha de la pantalla, aparecerá una ventana de información.
6. Lea la información y haga clic en el botón Crear al final de la ventana de información.
7. Rellene todos los campos necesarios. Utilice la información sobre las herramientas para obtener información y asistencia.
8. Al seleccionar el tamaño, seleccione una de las tres opciones destacadas.

   En la mayoría de los casos, 8 gigabytes (GB) de RAM son bastante. Sin embargo, en Azure, puede aumentar el tamaño de RAM y otros recursos de la máquina virtual en cualquier momento.
9. Al seleccionar una base de datos, seleccione una de las siguientes opciones, de acuerdo con su plan:

   - Local: si desea una base de datos en la misma máquina virtual en la que se instalará el Servidor de administración. Kaspersky Security Center viene con una base de datos SQL Server Express. Elija esta opción si SQL Server Express es suficiente para sus necesidades.
   - Nuevo: si desea una nueva base de datos de RDS en el entorno de Azure. Elija esta opción si desea un DBMS que no sea SQL Server Express. Sus datos se transferirán al entorno de nube, donde permanecerán y no tendrá ningún gasto adicional.
   - Existente: si desea utilizar un servidor de la base de datos existente. En este caso, tendrá que especificar su ubicación. Si este servidor está fuera del entorno de Azure, sus datos se transferirán a Internet, lo que podría causar gastos adicionales.
10. Al introducir el id. de la suscripción, utilice la suscripción que creó anteriormente.

Cuando concluya la instalación, podrá conectarse al Servidor de administración a través de RDP. Puede utilizar la Consola de administración para trabajar con el Servidor de administración.

# Trabajar con Azure SQL

Esta sección describe qué acciones se deben tomar para preparar una base de datos de Microsoft Azure para Kaspersky Security Center, preparar una cuenta de almacenamiento de Azure y migrar una base de datos existente a Azure SQL.

SQL Database es un servicio administrado de base de datos relacional de propósito general en Microsoft Azure.

Las direcciones de las páginas web que se mencionan en este documento eran válidas al momento de la publicación de Kaspersky Security Center.

## Creación de la cuenta de almacenamiento de Azure

Debe crear una cuenta de almacenamiento en Microsoft Azure para trabajar con la base de datos de Azure SQL y para los scripts de despliegue.

*Para crear una cuenta de almacenamiento:*

1. Inicie sesión en el portal de Azure.
2. En el recuadro izquierdo, seleccione **Cuentas de Almacenamiento** para ir a la ventana de **Cuentas de Almacenamiento**.
3. En la ventana **Cuentas de almacenamiento**, haga clic en el botón **Añadir** para proceder a la ventana **Crear cuenta de almacenamiento**.
4. Rellene todos los campos necesarios para crear una cuenta de almacenamiento:
   - Ubicación: debe ser la misma que la ubicación del Servidor de administración.
   - Otros campos: puede dejar los valores por defecto.

   Utilice la información sobre herramientas para obtener información sobre cada campo.

   Después de crear la cuenta de almacenamiento, se muestra la lista de sus cuentas de almacenamiento.
5. En la lista de sus cuentas de almacenamiento, haga clic en el nombre de la cuenta recién creada para ver información sobre esta cuenta.
6. Asegúrese de conocer el nombre de la cuenta, el grupo de recursos y las claves de acceso para esta cuenta de almacenamiento. Necesitará esta información para trabajar con Kaspersky Security Center.

Puede consultar el sitio web de Azure para obtener ayuda.

Si ya tiene una cuenta de almacenamiento, puede usarla para trabajar con Kaspersky Security Center.

## Creación de base de datos de SQL Azure y SQL Server

Necesita una base de datos de SQL y SQL Server en el entorno de Azure.

*Para crear una base de datos de SQL Azure y SQL Server:*

1. Siga las instrucciones sobre el sitio web de Azure.

   Puede crear un nuevo servidor cuando Microsoft Azure le pida que lo haga; si ya tiene un servidor SQL de Azure, puede usarlo para Kaspersky Security Center en lugar de crear uno nuevo.

2. Después de crear la base de datos de SQL y SQL Server, asegúrese que conoce el nombre del recurso y grupo del recurso:

   a. Vaya a https://portal.azure.com y constate que ha iniciado la sesión.

   b. En el panel izquierdo, **seleccione las bases de datos de SQL**.

   c. Haga clic en el nombre de la base de datos de la lista de sus bases de datos.

      Se abre la ventana de propiedades.

   d. El nombre de la base de datos es el nombre del recurso. El nombre del grupo de recursos se muestra en la sección **Información general** de la ventana Propiedades.

Necesita el nombre del recurso y el grupo del recurso de la base de datos para migrar la base de datos a Azure SQL.

## Migrar la base de datos a Azure SQL

Después del despliegue del Servidor de administración en el entorno de Azure, puede migrar su base de datos de Kaspersky Security Center desde un dispositivo local a Azure SQL. Necesita una cuenta de almacenamiento de Azure para una base de datos SQL de Azure. También debe tener el Marco de aplicación de nivel de datos de Microsoft SQL Server (DacFx) y SQLSysCLRTypes en su Servidor de administración.

*Para realizar la migración de la base de datos:*

1. Asegúrese de haber creado una cuenta de almacenamiento de Azure.

2. Asegúrese de que tenga SQLSysCLRTypes y DacFx en su Servidor de administración.

   Puede descargar el marco de aplicación de la capa de datos de Microsoft SQL Server (17.0.1 DacFx) y SQLSysCLRTypes (elija la versión que corresponda a la versión de su SQL Server) desde el sitio web oficial de Microsoft.

3. En su Servidor de administración físico (local), ejecute la utilidad Copia de seguridad de Kaspersky para hacer una copia de seguridad de los datos del Servidor de administración con la opción **Migrar al formato de Azure** habilitada.

4. Copiar la copia de seguridad al Servidor de administración de Azure.

   > Asegúrese de tener suficiente espacio en el disco en la máquina virtual de Azure donde está instalado el Servidor de administración. En el entorno de Azure, puede agregar espacio en disco a sus máquinas virtuales para adaptarse al proceso de migración de la base de datos.

5. En el Servidor de administración localizado en el entorno de Microsoft Azure, inicie nuevamente la utilidad de copia de seguridad de Kaspersky en modo interactivo.

   Se inicia el Asistente de copias de seguridad y restauración.

6. En el paso **Seleccione una acción**, seleccione **Restaurar datos del Servidor de administración** y haga clic en **Siguiente**.

7. En el paso **Opciones de restauración** de la restauración, pulse el botón **Examinar** al lado de la **Carpeta de almacenamiento de copias de seguridad**.

8. En la ventana **Inicie sesión en el almacenamiento en línea** que se abre, complete los siguientes campos y luego haga clic en **Aceptar**:

   - **Nombre de la cuenta de almacenamiento de Azure**

     Usted creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

   - **Carpeta de la copia de seguridad**

     Especifique la ubicación de la carpeta de almacenamiento que está destinada a la copia de seguridad.

   - **Id. de suscripción de Azure**

     Creó esta suscripción en el portal de Azure.

   - **Contraseña de la aplicación en Azure**

     Recibió la contraseña correspondiente al id. de aplicación cuando creó dicho id.

     Los caracteres de la contraseña se muestran como asteriscos. Cuando empiece a introducir la contraseña, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado para ver los caracteres introducidos.

   - **Clave de acceso al almacenamiento de Azure**

     Disponible en las propiedades de su cuenta de almacenamiento, en la sección Claves de acceso. Puede utilizar cualquiera de las claves (key1 o key2).

   - **Nombre del servidor SQL de Azure**

     Disponible en las propiedades de su servidor SQL de Azure.

   - **Grupo de recursos del servidor SQL de Azure**

     Disponible en las propiedades de su servidor SQL de Azure.

   - **Id. de la aplicación en Azure**

     Usted creó el id. de la aplicación en el portal de Azure.

     No puede especificar más de un id. de aplicación de Azure para realizar sondeos u otros fines. Si desea sondear otro segmento de Azure, elimine primero la conexión de Azure existente.

9. Seleccione la opción **Migrar desde la copia de seguridad local**.

   El botón **Examinar estará disponible**.

10. Pulse el botón **Examinar** para elegir la carpeta en el Servidor de administración de Azure donde copió la copia de seguridad.

11. Haga clic en **Siguiente** y complete el procedimiento.

    Sus datos se restaurarán en la base de datos SQL de Azure usando su almacenamiento de Azure. Puede usar esta base de datos para seguir trabajando con Kaspersky Security Center en el entorno de Azure.

Las direcciones de las páginas web que se mencionan en este documento eran válidas al momento de la publicación de Kaspersky Security Center.

# Trabajar con Google Cloud

Esta sección proporciona información sobre el trabajo con Kaspersky Security Center en un entorno de nube proporcionado por Google.

## Creación de correo electrónico de cliente, ID de proyecto y clave privada

Puede usar la API de Google para trabajar con Kaspersky Security Center en Google Cloud Platform. Necesitará una cuenta de Google. Para más detalles, consulte la documentación publicada por Google en https://cloud.google.com.

Deberá crear y proporcionar a Kaspersky Security Center las siguientes credenciales:

- **Correo electrónico del cliente**

  La dirección de correo electrónico que utilizó para registrar su proyecto en Google Cloud.

- **Id. de proyecto**

  El id. que le enviaron cuando registró su proyecto en Google Cloud.

- **Clave privada**

  La secuencia de caracteres que le enviaron como clave privada cuando registró su proyecto en Google Cloud. Recomendamos que copie y pegue esta secuencia para evitar errores.

# Trabajar con Google Cloud SQL para la instancia MySQL

Puede crear una base de datos en Google Cloud y usar esta base de datos para Kaspersky Security Center.

Kaspersky Security Center funciona con MySQL 5.7 y 5.6. No se han probado otras versiones de MySQL.

*Para crear y configurar una base de datos MySQL:*

En su navegador, vaya a https://cloud.google.com/sql/docs/mysql/create-instance#create-2nd-gen y siga las instrucciones proporcionadas.

Al configurar una base de datos MySQL, use las siguientes marcas:

- **sort_buffer_size** 10000000
- **join_buffer_size** 20000000
- **innodb_lock_wait_timeout** 300
- **max_allowed_packet** 32000000
- **innodb_thread_concurrency** 20
- **max_connections** 151
- **tmp_table_size** 67108864
- **max_heap_table_size** 67108864
- **lower_case_table_names** 1

# Requisitos previos para dispositivos cliente en un entorno de nube necesarios para trabajar con Kaspersky Security Center

Los dispositivos en los que pretende instalar el Servidor de administración, el Agente de red y las aplicaciones de seguridad de Kaspersky deben cumplir las siguientes condiciones:

- La configuración de los grupos de seguridad habilita los siguientes puertos en el Servidor de administración (conjunto mínimo de puertos necesarios para el despliegue):

  - 8060 HTTP: para transferir paquetes de instalación del Agente de red y paquetes de instalación de aplicaciones de seguridad desde el Servidor de administración a las instancias protegidas
  - 8061 HTTPS: para transferir paquetes de instalación del Agente de red y paquetes de instalación de aplicaciones de seguridad desde el Servidor de administración a las instancias protegidas
  - 13000 TCP: para realizar transferencias con SSL desde las instancias protegidas y los Servidores de administración secundarios al Servidor de administración principal
  - 13000 UDP: para transferir información sobre el cierre de instancias al Servidor de administración
  - 14000 TCP: para realizar transferencias desde las instancias protegidas y los Servidores de administración secundarios al Servidor de administración principal sin usar SSL
  - 13291: para conectar la Consola de administración con el Servidor de administración
  - 40080: para el funcionamiento de los scripts de despliegue

  Puede configurar los grupos de seguridad en la Consola de administración de AWS o en el portal de Azure. Si va a utilizar Kaspersky Security Center en una configuración no predeterminada, consulte la Base de conocimientos. Los ejemplos de configuraciones no predeterminadas no incluyen la instalación de la consola de administración en el dispositivo del Servidor de administración, pero sí instalarlo en su estación de trabajo en su lugar o el uso de un servidor proxy de KSN.

- El puerto 15000 UDP está abierto en los dispositivos cliente (para recibir solicitudes de comunicación con el Servidor de administración).

- En el entorno de nube de AWS:
  - Si planea usar la API de AWS, la función de IAM se establece bajo la cual se instalarán las aplicaciones en las instancias.
  - En cada instancia de Amazon EC2, el Agente de Systems Manager (Agente de SSM) está instalado y en ejecución.
  - El Agente de SSM activa Kaspersky Security Center para instalar automáticamente aplicaciones en dispositivos y grupos de dispositivos sin solicitar confirmación por un administrador cada vez.
  - En las instancias que ejecuten un sistema operativo Windows y que se hayan instalado a partir de una AMI con posterioridad a noviembre de 2016, el Agente de SSM estará instalado y en funcionamiento. Tendrá que instalar manualmente el Agente de SSM en todos otros dispositivos. Para obtener más información sobre la instalación del Agente de SSM en dispositivos que ejecutan sistemas operativos de Windows y Linux, consulte la página de Ayuda de AWS.
- En el entorno de nube de Microsoft Azure:
  - En cada máquina virtual de Azure, Agente de VM de Azure está instalado y en ejecución.

    De forma predeterminada, se crea una nueva máquina virtual con el Agente de VM de Azure y no tiene que instalarla o habilitarla manualmente. Consulte las páginas de Ayuda de Microsoft para obtener detalles sobre el Agente de VM de Azure en dispositivos Windows y en dispositivos Linux.
  - El Id. de aplicación de Azure tiene las siguientes funciones:
    - Lector (para detectar máquinas virtuales mediante el uso de sondeos)
    - Colaborador de máquina virtual (para desplegar la protección en las máquinas virtuales)
    - Colaborador de SQL Server (para usar una base de datos SQL en el entorno de Microsoft Azure)

    Si desea realizar todas estas operaciones, asigne las tres funciones al id. de aplicación de Azure.

# Creación de los paquetes de instalación necesarios para configurar el entorno de nube

El Asistente de configuración del entorno de nube en Kaspersky Security Center está disponible si tiene los paquetes de instalación y los complementos de administración para los siguientes programas:

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security para Windows

  El despliegue de Kaspersky Endpoint Security para Windows en un entorno de nube estará disponible después del próximo lanzamiento de Kaspersky Endpoint Security 12.0 para Windows.
- Kaspersky Security for Windows Server

Estos paquetes de instalación son necesarios para instalar las aplicaciones en las instancias o máquinas virtuales que desea proteger. Si no tiene estos paquetes de instalación, debe crearlos. De lo contrario, el Asistente de configuración del entorno de nube no puede funcionar.

Para crear los paquetes de instalación:

1. Descargue las versiones más recientes de las aplicaciones y los complementos en el sitio web de Kaspersky:
   - El instalador y el complemento de administración para Kaspersky Security for Windows Server.
   - El instalador, los archivos para la instalación remota a través de Kaspersky Security Center, y el complemento de administración para Kaspersky Endpoint Security for Linux.
2. Guarde todos los archivos en la instancia (o la máquina virtual) donde está instalado el Servidor de administración.
3. Extraiga los archivos de todos los paquetes.
4. Inicie Kaspersky Security Center.
5. En el árbol de la consola, vaya a **Avanzado** → **Instalación remota** → **Paquetes de instalación** y haga clic en **Crear paquete de instalación**.
6. Seleccione **Crear paquete de instalación de Kaspersky**.
7. Especifique el nombre del paquete y la ruta hacia el instalación de la aplicación: <carpeta>\<nombre de archivo>.kud. A continuación, haga clic en **Siguiente**.
8. Lea el Contrato de licencia de usuario final y seleccione la casilla de verificación para confirmar que acepta sus términos. A continuación, haga clic en **Siguiente**.

El paquete de instalación se cargará en el Servidor de administración y estará disponible en la lista de paquetes de instalación.

La configuración de un entorno de nube está disponible en cuanto se crean los paquetes de instalación y se instalan los complementos de administración en el Servidor de administración.

# Configuración del entorno de nube

Para configurar Kaspersky Security Center mediante el Asistente de configuración del entorno de nube, debe tener lo siguiente:

- Las credenciales específicas de un entorno de nube:
  - Una función de IAM a la que se le haya otorgado el derecho de sondear el segmento de la nube o una cuenta de usuario de IAM a la que se le haya otorgado el derecho de sondear el segmento de la nube (para trabajar con Amazon Web Services)
  - Id. de aplicación, contraseña y suscripción de Azure (para operar con Microsoft Azure)
  - Correo electrónico del cliente, id. de proyecto y clave privada de Google (para operar con Google Cloud)
- Paquetes de instalación:
  - Agente de red para Windows
  - Agente de red para Linux
  - Kaspersky Endpoint Security for Linux
- Complemento web para Kaspersky Endpoint Security for Linux
- Al menos uno de los siguientes:
  - Paquete de instalación y complemento web para Kaspersky Endpoint Security para Windows (recomendado)
  - Paquete de instalación y complemento de administración de Kaspersky Security for Windows Server

Si no desea usar capacidades del entorno de nube (si, por ejemplo, desea administrar la protección de dispositivos cliente físicos solamente), puede cerrar el Asistente de configuración del entorno de nube y ejecutar el Asistente de inicio rápido del Servidor de administración manualmente.

Si realiza el despliegue de Kaspersky Security Center con una imagen lista para usar, la Configuración del entorno de nube se abrirá automáticamente cuando se conecte al Servidor de administración por primera vez a través de la Consola de administración. Además, puede iniciar el Asistente de configuración del entorno de nube manualmente en cualquier momento.

*Para iniciar el Asistente de configuración del entorno de nube manualmente:*

1. En el árbol de consola, haga clic el nodo del **Servidor de administración**.
2. En el menú contextual del nodo, seleccione **Todas las tareas** → **Configurar entorno de nube**.

La sesión de trabajo promedio dura unos 15 minutos.

# Acerca del asistente de configuración del entorno de nube

El Asistente de configuración del entorno de nube le permite configurar Kaspersky Security Center teniendo en cuenta las particularidades de trabajar en un entorno de nube.

El asistente crea los siguientes objetos:

- Directiva de Agente de red con configuraciones predeterminadas
- Directiva para Kaspersky Endpoint Security para Linux
- Directiva para Kaspersky Security for Windows Server
- Grupo de administración para instancias y una regla para mover automáticamente instancias a este grupo de administración
- Tarea de copia de seguridad de datos del Servidor de administración
- Tareas para instalar la protección en dispositivos que ejecutan Linux y Windows
- Tareas para cada dispositivo administrado:
  - Análisis antimalware rápido
  - Descarga de actualización

Si seleccionó la opción de licencias BYOL, la configuración del entorno de nube también activa Kaspersky Security Center con un archivo de clave o código de activación en el almacenamiento de la licencia.

# Paso 1. Selección del método de activación de la aplicación

Este paso no se muestra si se registró en una de las AMI listas para usar (en AWS Marketplace) o en una SKU facturada mensualmente según el uso (en Azure Marketplace). En este caso, el Asistente pasa inmediatamente al siguiente paso. Sin embargo, no puede comprar una AMI lista para usar para Google Cloud.

Si seleccionó la opción de licencia BYOL para Kaspersky Security Center, el Asistente le solicitará que seleccione el método de activación de la aplicación.

Activar la aplicación con un código de activación (o archivo de clave) para Kaspersky Security for Virtualization o para la Seguridad de la nube del híbrido de Kaspersky.

Puede activar la aplicación de una de las siguientes maneras:

- Al escribir un código de activación.

  Se inicia la activación en línea. Este procesó implicará la verificación del código de activación especificado, así como de la emisión y activación del archivo de clave.

- Especificando un archivo de clave.

  La aplicación comprobará el archivo de clave y lo activará si contiene información correcta, o le solicitará especificar otro archivo de clave.

Kaspersky Security Center guardará la clave de licencia en el repositorio de licencias y la marcará como distribuida automáticamente a los dispositivos administrados.

Si se conecta a una instancia usando la conexión de escritorio remoto estándar en Microsoft Windows o una aplicación similar, en las propiedades de conexión remota tiene que especificar la unidad del dispositivo físico que está utilizando para conectarse. Esto asegura el acceso desde la instancia a los archivos en su dispositivo físico y le permite seleccionar y especificar el archivo de clave.

Si trabaja con Kaspersky Security Center desplegado desde una AMI pagada o para un SKU que se facture según uso, no puede agregar archivos de clave ni códigos de activación al almacenamiento de la licencia.

## Paso 2. Selección del entorno de nube

Seleccione el entorno de nube en el que va a realizar el despliegue de Kaspersky Security Center: AWS, Azure o Google Cloud.

## Paso 3. Autorización en el entorno de nube

### AWS

Si seleccionó AWS, debe especificar que tiene una función de IAM con los derechos requeridos o debe proporcionar a Kaspersky Security Center una clave de acceso de AWS IAM. El sondeo del segmento de la nube no es posible sin una función de IAM o una clave de acceso de AWS IAM.

Configure los siguientes ajustes para la conexión que se utilizará para seguir sondeando el segmento de la nube:

- **Nombre de la conexión**

  Escriba un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres Unicode.

  El nombre que escriba aquí será también el nombre del grupo de administración para los dispositivos de nube.

  Si planea trabajar con más de un entorno de nube, sugerimos que incluya el nombre del entorno en el nombre de la conexión (por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google").

- **Usar función de AWS IAM**

  Elija esta opción si ha creado ya una función de IAM para que el Servidor de administración use servicios AWS.

- **Usar cuenta de usuario de AWS IAM**

  Seleccione esta opción si tiene una cuenta de usuario de IAM con los permisos necesarios y puede ingresar un id. de clave y una clave secreta.

  - **Id. de clave de acceso**

    El id. de la clave de acceso de IAM es una secuencia de caracteres alfanuméricos. Obtuvo este id. al crear la cuenta de usuario de IAM.

    El campo está disponible si seleccionó una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

  - **Clave secreta**

    La clave secreta que recibió con el id. de la clave de acceso al crear la cuenta de usuario de IAM.

    Los caracteres de la clave secreta se muestran como asteriscos. Cuando comience a escribir la clave secreta, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado el tiempo que necesite para ver los caracteres introducidos.

    El campo está disponible si seleccionó una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

Esta conexión se guarda en la configuración de la aplicación. Puede crear una única clave de acceso de IAM de AWS con Configurar entorno de nube. Posteriormente, puede especificar más conexiones para administrar otros segmentos de la nube.

Si desea instalar aplicaciones en instancias mediante Kaspersky Security Center, debe asegurarse de que su función de IAM (o el usuario de IAM cuya cuenta esté asociada con la clave que está ingresando) tenga todos los permisos requeridos.

## Azure

Si seleccionó Azure, especifique la siguiente configuración para la conexión que se usará para un sondeo adicional del segmento de la nube:

- **Nombre de la conexión**

  Escriba un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres Unicode.

  El nombre que escriba aquí será también el nombre del grupo de administración para los dispositivos de nube.

  Si planea trabajar con más de un entorno de nube, sugerimos que incluya el nombre del entorno en el nombre de la conexión (por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google").

- **Id. de la aplicación en Azure**

  Usted creó el id. de la aplicación en el portal de Azure.

  No puede especificar más de un id. de aplicación de Azure para realizar sondeos u otros fines. Si desea sondear otro segmento de Azure, elimine primero la conexión de Azure existente.

- **Id. de suscripción de Azure**

  Creó esta suscripción en el portal de Azure.

- **Contraseña de la aplicación en Azure**

  Recibió la contraseña correspondiente al id. de aplicación cuando creó dicho id.

  Los caracteres de la contraseña se muestran como asteriscos. Cuando empiece a introducir la contraseña, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado para ver los caracteres introducidos.

- **Nombre de la cuenta de almacenamiento de Azure**

  Usted creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

- **Clave de acceso al almacenamiento de Azure**

  Recibió una contraseña (clave) cuando creó la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

  La clave está disponible en la sección "Overview of the Azure storage account" ("Descripción general de la cuenta de almacenamiento de Azure"), subsección "Keys" ("Claves").

Esta conexión se guarda en la configuración de la aplicación.

### Google Cloud

Si seleccionó Google Cloud, especifique la siguiente configuración para la conexión que se usará para un sondeo adicional del segmento de la nube:

- **Nombre de conexión**

  Escriba un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres Unicode.

  El nombre que escriba aquí será también el nombre del grupo de administración para los dispositivos de nube.

  Si planea trabajar con más de un entorno de nube, sugerimos que incluya el nombre del entorno en el nombre de la conexión (por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google").

- **Correo electrónico del cliente**

  La dirección de correo electrónico que utilizó para registrar su proyecto en Google Cloud.

- **Id. de proyecto**

  El id. que le enviaron cuando registró su proyecto en Google Cloud.

- **Clave privada**

  La secuencia de caracteres que le enviaron como clave privada cuando registró su proyecto en Google Cloud. Recomendamos que copie y pegue esta secuencia para evitar errores.

Esta conexión se guarda en la configuración de la aplicación.

## Paso 4. Configuración de la sincronización con Cloud y elección de otras acciones

En este paso, se inicia el sondeo del segmento de la nube y se crea un grupo de administración especial para las instancias. Se aplican las instancias encontradas durante el sondeo. La programación de votación de segmento de la nube se configura (cada 5 minutos de forma predeterminada).

La aplicación también creará una regla de movimiento automático llamada **Sincronizar con la nube**. Para cada análisis posterior de la red en la nube, los dispositivos virtuales detectados se moverán al subgrupo correspondiente dentro del grupo **Dispositivos administrados\Nube**.

En la página **Sincronización con el segmento de la nube**, puede definir la siguiente configuración:

- **Sincronizar la estructura del grupo de administración con el segmento de la nube**

  Si habilita está opción, se creará el grupo **Cloud** automáticamente dentro el grupo **Dispositivos administrados** y se iniciará un proceso para descubrir dispositivos en la nube. Las instancias y las máquinas virtuales que se detecten cada vez que se sondee la red de la nube se agregarán al grupo "Cloud". La estructura de subgrupos de administración dentro de este grupo se hará coincidir con la estructura del segmento de la nube (en AWS, las zonas de disponibilidad y los grupos de ubicación no estarán representados en la estructura; en Azure, no estarán representadas las subredes). Los dispositivos que no se hayan identificado como instancias en el entorno de nube estarán en el grupo **Dispositivos no asignados**. Esta estructura de grupo le permite usar tareas de instalación en grupo para instalar aplicaciones antivirus en instancias, así como configurar diferentes directivas para diferentes grupos.

  Si no habilita esta opción, también se creará el grupo **Cloud** y también se iniciará el descubrimiento de dispositivos de la nube, pero no se crearán subgrupos que coincidan con la estructura del segmento de la nube dentro del grupo. Todas las instancias detectadas se agregarán al grupo de administración **Cloud** y aparecerán en una misma lista. Si su trabajo con Kaspersky Security Center requiere sincronización, puede modificar las propiedades de la regla **Sincronizar con Cloud** y aplicarla. Al aplicar la regla, la estructura de subgrupos del grupo "Cloud" se hará coincidir con la estructura del segmento de la nube.

  Esta opción está deshabilitada de forma predeterminada.

- **Desplegar protección**

  Si se selecciona esta opción, el asistente crea una tarea para instalar aplicaciones de seguridad en instancias. Una vez que finalice el asistente, el Asistente de despliegue de la protección se inicia automáticamente en los dispositivos de sus segmentos de nube, y usted podrá instalar el Agente de red y las aplicaciones de seguridad en esos dispositivos.

  Kaspersky Security Center puede realizar el despliegue con sus herramientas nativas. Si no tiene permisos para instalar las aplicaciones en instancias EC2 o máquinas virtuales de Azure, puede configurar la tarea **Instalación remota** manualmente y especificar una cuenta con los permisos requeridos. En este caso, la tarea de instalación remota no funcionará para los dispositivos detectados utilizando la API de AWS o Azure. Esta tarea solo funciona para los dispositivos descubiertos mediante el sondeo de Active Directory, el sondeo de dominios de Windows o el sondeo de rango de IP.

  Si esta opción no está seleccionada, el Asistente de despliegue de la protección no se inicia y no se crean tareas para instalar las aplicaciones de seguridad en las instancias. Puede realizar manualmente ambas acciones más adelante.

Para Google Cloud, solo puede realizar el despliegue con herramientas propias de Kaspersky Security Center. Si seleccionó Google Cloud, la opción **Desplegar protección** no estará disponible.

## Paso 5. Configuración de Kaspersky Security Network en el entorno de nube

Especifique la configuración para transmitir la información sobre operaciones Kaspersky Security Center a la base de conocimientos de Kaspersky Security Network. Seleccione una de las siguientes opciones:

- **Acepto utilizar Kaspersky Security Network**

  Kaspersky Security Center y las aplicaciones administradas instaladas en dispositivos cliente transferirán automáticamente su información de operación a Kaspersky Security Network. Participar en Kaspersky Security Network permite que las bases de datos con información sobre virus y otros riesgos se actualicen más rápidamente, lo cual se traduce en una mayor velocidad de respuesta ante amenazas a la seguridad emergentes.

- **No acepto utilizar Kaspersky Security Network**

  Kaspersky Security Center y las aplicaciones administradas no proporcionarán información a Kaspersky Security Network.

  Si selecciona esta opción, se deshabilitará el uso de Kaspersky Security Network.

Kaspersky recomienda participar en Kaspersky Security Network.

## Paso 6. Configuración de notificaciones por correo electrónico en el entorno de nube

Configure el envío de notificaciones sobre eventos registrados durante el funcionamiento de aplicaciones Kaspersky en los dispositivos cliente virtuales. Estos parámetros servirán de configuración predeterminada de las directivas de la aplicación.

Para configurar la entrega de notificaciones sobre eventos que ocurren en Aplicaciones de Kaspersky, use la configuración siguiente:

- **Destinatarios (direcciones de correo electrónico)**

  Las direcciones de correo electrónico de usuarios a quien la aplicación enviará notificaciones. Puede ingresar una o más direcciones; si ingresa más de una dirección, sepárelas con un punto y coma.

- **Servidores SMTP**

  La dirección o direcciones de los servidores de correo de su organización.

  Si ingresa más de una dirección, sepárelas con un punto y coma. Puede utilizar los siguientes parámetros:

  - Dirección IPv4 o IPv6
  - Nombre de la red de Windows (nombre NetBIOS) del dispositivo
  - Nombre DNS del servidor SMTP

- **Puerto de los servidores SMTP**

  Número del puerto de comunicación del servidor SMTP. Si utiliza varios servidores SMTP, la conexión con ellos se establecerá a través del puerto de comunicación especificado. El número de puerto predeterminado es 25.

- **Utilizar autenticación ESMTP**

  Habilita la compatibilidad con la autenticación ESMTP. Cuando la casilla está seleccionada, en los campos **Nombre de usuario** y **Contraseña**, puede especificar la configuración de la autorización de ESMTP. Esta casilla no está marcada de manera predeterminada.

Puede probar la configuración de la notificación por correo electrónico nueva haciendo clic en el botón **Enviar mensaje de prueba**. Si el mensaje de prueba se recibiera correctamente en las direcciones especificadas en el campo **Destinatarios (direcciones de correo electrónico)**, la configuración se ha realizado correctamente.

## Paso 7. Creación de una configuración inicial de la protección del entorno de nube

En este paso, Kaspersky Security Center automáticamente crea directivas y tareas. La ventana **Configuración inicial de la protección** muestra una lista de directivas y tareas creadas por la aplicación.

Si utiliza una base de datos de RDS en el entorno de nube de AWS, debe proporcionar el par de claves de acceso de IAM a Kaspersky Security Center cuando se está creando la tarea de copia de seguridad del Servidor de administración. En este caso, rellene los siguientes campos:

- **Nombre del bucket de S3**

  El nombre del bucket de S3 que creó para la copia de seguridad.

- **Id. de clave de acceso**

  Recibió el id. de clave (secuencia de caracteres alfanuméricos) cuando creó la cuenta de usuario de IAM para trabajar con la instancia de almacenamiento en buckets de S3.

  El campo está disponible si ha seleccionado la base de datos de RDS en un bucket de S3.

- **Clave secreta**

  La clave secreta que recibió con el id. de la clave de acceso al crear la cuenta de usuario de IAM.

  Los caracteres de la clave secreta se muestran como asteriscos. Cuando comience a escribir la clave secreta, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado el tiempo que necesite para ver los caracteres introducidos.

  El campo está disponible si seleccionó una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

Si utiliza una base de datos SQL de Azure en el entorno de nube de Azure, debe proporcionar información sobre su servidor SQL de Azure a Kaspersky Security Center cuando se cree la tarea de copia de seguridad del Servidor de administración. En este caso, rellene los siguientes campos:

- **Nombre de la cuenta de almacenamiento de Azure**

  Usted creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

- **Id. de suscripción de Azure**

  Creó esta suscripción en el portal de Azure.

- **Contraseña de la aplicación en Azure**

  Recibió la contraseña correspondiente al id. de aplicación cuando creó dicho id.

  Los caracteres de la contraseña se muestran como asteriscos. Cuando empiece a introducir la contraseña, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado para ver los caracteres introducidos.

- **Id. de la aplicación en Azure**

  Usted creó el id. de la aplicación en el portal de Azure.

  No puede especificar más de un id. de aplicación de Azure para realizar sondeos u otros fines. Si desea sondear otro segmento de Azure, elimine primero la conexión de Azure existente.

- **Nombre del servidor SQL de Azure**

  El nombre y el grupo de recursos están disponibles en las propiedades del Servidor SQL de Azure.

- **Grupo de recursos del servidor SQL de Azure**

  El nombre y el grupo de recursos están disponibles en las propiedades del Servidor SQL de Azure.

- **Clave de acceso al almacenamiento de Azure**

  Disponible en las propiedades de su cuenta de almacenamiento, en la sección Claves de acceso. Puede utilizar cualquiera de las claves (key1 o key2).

Si el Servidor de administración va a estar instalado en Google Cloud, debe seleccionar la carpeta en la que se guardarán las copias de seguridad. Seleccione una carpeta en su dispositivo local o una carpeta en una instancia de máquina virtual.

El botón **Siguiente** queda disponible después de la creación de todas las directivas y tareas que son necesarias para la configuración mínima de la protección.

Si un dispositivo en el que se supone que las tareas deben ejecutarse no es visible para el Servidor de administración, las tareas se inician solo cuando el dispositivo se vuelve visible. Si crea una nueva instancia de EC2 o una nueva máquina virtual de Azure, puede tomar algún tiempo antes de que sea visible para el Servidor de administración. Si desea que el Agente de red y las aplicaciones de seguridad se instalen en todos los dispositivos recién creados tan pronto como sea posible, asegúrese de que la opción **Ejecutar tareas pendientes** esté activada para las tareas de **Instalación remota de la aplicación**. De lo contrario, una instancia/máquina virtual recién creada no obtendrá el Agente de red y las aplicaciones de seguridad hasta que la tarea comience de acuerdo con su programación.

## Paso 8. Selección de la acción cuando el sistema operativo se debe reiniciar durante la instalación (para el entorno de nube)

Si seleccionó anteriormente la opción **Desplegar protección**, debe elegir qué hacer cuando se deba reiniciar el sistema operativo de un dispositivo de destino. Si no seleccionó la opción **Desplegar protección**, este paso se omitirá.

Seleccione si reiniciar instancias si el sistema operativo de su dispositivo debe reiniciarse durante la instalación de aplicaciones:

- **No reiniciar el dispositivo**

  Si se selecciona esta opción, el dispositivo no se reiniciará después de instalar la aplicación de seguridad.

- **Reiniciar el dispositivo**

  Si se selecciona esta opción, el dispositivo se reiniciará después de instalar la aplicación de seguridad.

Si desea forzar el cierre de todas las aplicaciones en sesiones bloqueadas en las instancias antes del reinicio, seleccione la casilla **Forzar el cierre de aplicaciones en sesiones bloqueadas**. Si se desactiva esta casilla, deberá cerrar manualmente todas las aplicaciones que se ejecutan en instancias bloqueadas.

## Paso 9. Recepción de actualizaciones por un Servidor de administración

En este paso, puede consultar el progreso de descargar actualizaciones necesarias para la operación correcta del Servidor de administración. Puede hacer clic en el botón **Siguiente** sin esperar a que finalice la descarga, para continuar a la página final del Asistente.

El Asistente finaliza.

# Comprobación de la configuración

*Para comprobar si Kaspersky Security Center 15.1 está correctamente configurado para funcionar en el entorno de nube, realice lo siguiente:*

1. Inicie Kaspersky Security Center y asegúrese de que puede conectarse al Servidor de administración a través de la Consola de administración.

2. En el árbol de consola, seleccione **Dispositivos administrados\Cloud**.

3. Al ver a cualquier de los subgrupos en el grupo **Dispositivos administrados\Cloud**, asegúrese de que la pestaña **Dispositivos** muestre todas los dispositivos de ese subgrupo.

   Si no se muestran los dispositivos, puede sondear manualmente los segmentos de la nube correspondientes para encontrarlos.

4. Asegúrese que la pestaña **Directivas** tenga directivas activas para las siguientes aplicaciones:

   - Agente de red de Kaspersky Security Center
   - Kaspersky Security for Windows Server
   - Kaspersky Endpoint Security for Linux

   Si no están en la lista, puede crearlos manualmente.

5. Asegúrese de que la pestaña **Tareas** contenga las siguientes tareas:

   - **Copia de seguridad de los datos del Servidor de administración**
   - **Tarea de actualización para Windows Server**
   - **Mantenimiento del Servidor de administración**
   - **Descargar actualizaciones en el repositorio del Servidor de administración**
   - **Buscar vulnerabilidades y actualizaciones requeridas**
   - **Instalar protección para Windows**
   - **Instalar protección para Linux**
   - **Tarea de análisis rápido para Windows Server**
   - **Análisis rápido**
   - **Instalar actualizaciones para Linux**

   Si no están en la lista, puede crearlos manualmente.

Kaspersky Security Center 15.1 está correctamente configurado para funcionar en el entorno de nube.

# Grupo de dispositivos de nube

Puede administrar dispositivos en la nube combinándolos en grupos. En la etapa de configuración inicial de Kaspersky Security Center, se crea el grupo de administración **Dispositivos administrados\Nube** de forma predeterminada y los dispositivos en la nube detectados durante el sondeo se colocan en este grupo.

Si seleccionó la opción **Sincronizar la estructura del grupo de administración con el segmento de la nube** de la nube cuando configuró la sincronización, la estructura de los subgrupos en este grupo de administración es idéntica a la estructura de sus segmentos de nube. (Sin embargo, en AWS, las zonas de disponibilidad y los grupos de ubicación no están representados en la estructura; en Microsoft Azure, las subredes no están representadas en la estructura). Los subgrupos vacíos dentro del grupo que se detecten durante el sondeo se eliminan automáticamente.

También puede crear manualmente grupos de administración al combinar todas las instancias o dispositivos específicos.

De forma predeterminada, el grupo **Dispositivos administrados\Nube** hereda las directivas y tareas desde el grupo de **Dispositivos administrados**. Puede cambiar la configuración si la casilla **Edición permitida** se selecciona en las propiedades de la configuración de las directivas correspondientes y tareas.

# Sondeo de segmentos de red

Información sobre la estructura de la red y dispositivos en esta red se recibe por el Servidor de administración a través del sondeo habitual de segmentos de la nube usando herramientas de API de AWS o API de Azure o API de Google. Kaspersky Security Center usa esta información para actualizar el contenido de las carpetas **Dispositivos no asignados** y **Dispositivos administrados**. Si configuró dispositivos para que se trasladen de forma automática a grupos de administración, los dispositivos detectados se incluirán en los grupos de administración.

Para sondear segmentos de nube, el Servidor de administración necesitará contar con ciertos derechos, que pueden otorgarse a través de una función de IAM o una cuenta de usuario de IAM (si el proveedor es AWS), un id. de la aplicación y la contraseña de esa aplicación (si el proveedor es Azure) o un id. de proyecto, una clave privada y el correo electrónico del cliente (si el proveedor es Google).

Puede agregar y eliminar conexiones, así como configurar la programación de sondeo para cada segmento de la nube.

## Adición de conexiones para el sondeo de segmento de la nube

*Para agregar una conexión para sondear un segmento de nube a la lista de conexiones disponibles:*

1. En el árbol de consola, seleccione el nodo **Descubrimiento de dispositivos** → **Cloud**.
2. En el espacio de trabajo de la ventana, haga clic en **Configurar sondeo**.

   Se abre una ventana de propiedades que contiene una lista de conexiones disponibles para el sondeo de segmento de la nube.
3. Haga clic en el botón **Agregar**.

   Se abre la ventana **Conexión**.

4. Escriba el nombre del entorno de nube correspondiente a la conexión que se usará para sondear el segmento de nube:

**Entorno de nube**

El entorno en el que se encuentren las instancias de EC2 (o las máquinas virtuales) puede ser Amazon Web Services (AWS), Microsoft Azure o Google Cloud.

Si seleccionó AWS, configure los siguientes parámetros:

- **Nombre de la conexión**

  Escriba un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres Unicode.

  El nombre que escriba aquí será también el nombre del grupo de administración para los dispositivos de nube.

  Si planea trabajar con más de un entorno de nube, sugerimos que incluya el nombre del entorno en el nombre de la conexión (por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google").

- **Usar función de AWS IAM**

  Elija esta opción si ha creado ya una función de IAM para que el Servidor de administración use servicios AWS.

- **Usar cuenta de usuario de AWS IAM**

  Seleccione esta opción si tiene una cuenta de usuario de IAM con los permisos necesarios y puede ingresar un id. de clave y una clave secreta.

  - **Id. de clave de acceso**

    El id. de la clave de acceso de IAM es una secuencia de caracteres alfanuméricos. Obtuvo este id. al crear la cuenta de usuario de IAM.

    El campo está disponible si seleccionó una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

  - **Clave secreta**

    La clave secreta que recibió con el id. de la clave de acceso al crear la cuenta de usuario de IAM.

    Los caracteres de la clave secreta se muestran como asteriscos. Cuando comience a escribir la clave secreta, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado el tiempo que necesite para ver los caracteres introducidos.

    El campo está disponible si seleccionó una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

El Asistente de configuración del entorno de nube le permite especificar únicamente una sola clave de acceso de AWS IAM. Posteriormente, puede especificar más conexiones para administrar otros segmentos de la nube.

Si seleccionó Azure, configure los siguientes parámetros:

- **Nombre de la conexión**

  Escriba un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres Unicode.

  El nombre que escriba aquí será también el nombre del grupo de administración para los dispositivos de nube.

  Si planea trabajar con más de un entorno de nube, sugerimos que incluya el nombre del entorno en el nombre de la conexión (por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google").

- **Id. de la aplicación en Azure**

  Usted creó el id. de la aplicación en el portal de Azure.

  No puede especificar más de un id. de aplicación de Azure para realizar sondeos u otros fines. Si desea sondear otro segmento de Azure, elimine primero la conexión de Azure existente.

- **Id. de suscripción de Azure**

  Creó esta suscripción en el portal de Azure.

- **Contraseña de la aplicación en Azure**

  Recibió la contraseña correspondiente al id. de aplicación cuando creó dicho id.

  Los caracteres de la contraseña se muestran como asteriscos. Cuando empiece a introducir la contraseña, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado para ver los caracteres introducidos.

- **Nombre de la cuenta de almacenamiento de Azure**

  Usted creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

- **Clave de acceso al almacenamiento de Azure**

  Recibió una contraseña (clave) cuando creó la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

  La clave está disponible en la sección "Overview of the Azure storage account" ("Descripción general de la cuenta de almacenamiento de Azure"), subsección "Keys" ("Claves").

Si seleccionó Google Cloud, configure los siguientes ajustes:

- **Nombre de la conexión**

Escriba un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres Unicode.

El nombre que escriba aquí será también el nombre del grupo de administración para los dispositivos de nube.

Si planea trabajar con más de un entorno de nube, sugerimos que incluya el nombre del entorno en el nombre de la conexión (por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google").

- **Correo electrónico del cliente**

  La dirección de correo electrónico que utilizó para registrar su proyecto en Google Cloud.

- **Id. de proyecto**

  El id. que le enviaron cuando registró su proyecto en Google Cloud.

- **Clave privada**

  La secuencia de caracteres que le enviaron como clave privada cuando registró su proyecto en Google Cloud. Recomendamos que copie y pegue esta secuencia para evitar errores.

5. Si lo desea, seleccione **Establecer programación de sondeo** y cambiar la configuración predeterminada.

   La conexión se guarda en la configuración de la aplicación.

Una vez que el nuevo segmento de la nube se haya sondeado por primera vez, el subgrupo correspondiente a ese segmento aparecerá en el grupo de administración **Dispositivos administrados\Nube**.

Si las credenciales que introdujo no son correctas, no se encontrará ninguna instancia durante el sondeo del segmento y, en consecuencia, no aparecerá ningún subgrupo nuevo en el grupo de administración **Dispositivos administrados\Cloud**.

## Eliminación de conexiones para el sondeo de segmento de la nube

Si ya no tiene que sondear un segmento de la nube específico, puede eliminar la conexión correspondiente a ese segmento de la lista de claves disponibles. También puede eliminar una conexión si, por ejemplo, los permisos para sondear un segmento de la nube se han transferido a otro usuario de AWS IAM con una clave diferente.

*Para eliminar una conexión:*

1. En el árbol de consola, seleccione el nodo **Descubrimiento de dispositivos** → **Cloud**.

2. En el espacio de trabajo de la ventana, seleccione **Configurar sondeo**.

   Se abre una ventana que contiene una lista de conexiones disponibles para el sondeo de segmento de la nube.

3. Seleccione la conexión que desea eliminar y haga clic en el botón **Eliminar** en la parte derecha de la ventana.

4. En la ventana que se abre, haga clic en el botón **Aceptar** para confirmar su selección.

Si está eliminando conexiones de la lista de conexiones disponibles, los dispositivos que se encuentran en los segmentos correspondientes se eliminan automáticamente de los grupos de administración correspondiente.

## Configuración de la programación de sondeos

El sondeo de segmentos de nube se realiza siguiendo una programación. Si lo desea, puede configurar la frecuencia con la que se llevan a cabo los sondeos.

La frecuencia de sondeo se establece automáticamente en 5 minutos en la configuración del entorno de nube. Puede cambiar este valor en cualquier momento y definir una programación diferente. Sin embargo, no se recomienda configurar el sondeo para que se ejecute con más frecuencia que cada 5 minutos, porque esto podría llevar a errores en la operación API.

*Para configurar la programación de sondeo para un segmento de nube:*

1. En el árbol de consola, seleccione el nodo **Descubrimiento de dispositivos** → **Nube**.

2. En el espacio de trabajo, haga clic en **Configurar sondeo**.

   Se abre la ventana de propiedades de nube.

3. En la lista, seleccione la conexión que desea y haga clic en el botón **Propiedades**.

   Se abre la ventana de propiedades de la conexión.

4. En la ventana de propiedades, haga clic en **Establecer programación de sondeo**.

   Se abre la ventana **Programación**.

5. Defina los siguientes parámetros de configuración:

- **Inicio programado**

  Opciones de programación para el sondeo:

  - Cada N días

    Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la fecha y hora indicadas. Cada sondeo estará separado del anterior por el número de días que indique.

    De forma predeterminada, se realizará un sondeo todos los días, a partir de la fecha y hora actuales del sistema.

  - Cada N minutos

    Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la hora indicada. Cada sondeo estará separado del anterior por el número de minutos que indique.

    De forma predeterminada, se realizará un sondeo cada cinco minutos, a partir de la hora actual del sistema.

  - Por días de la semana

    Se realizará un sondeo en forma periódica, a intervalos regulares, en el día de la semana y a la hora que indique.

    De manera predeterminada, el sondeo se ejecutará todos los viernes a las 18:00:00.

  - Cada mes en los días especificados de semanas seleccionadas

    Se realizará un sondeo en forma periódica, a intervalos regulares, en los días del mes y a la hora que indique.

    Por defecto, no hay ningún día seleccionado; la hora de inicio predeterminada es las 18:00:00.

- Ejecutar tareas no realizadas

  Si el Servidor de administración está apagado o no está disponible durante la hora programada para el sondeo, el Servidor de administración puede iniciar el sondeo inmediatamente después de encenderlo o esperar la próxima vez que se programe el sondeo.

  Si esta opción está habilitada, el Servidor de administración inicia el sondeo inmediatamente después de que se enciende.

  Si esta opción está desactivada, el Servidor de administración espera la próxima vez que se programe el sondeo.

  Esta opción está activada de forma predeterminada.

6. Haga clic en **Aceptar** para guardar los cambios.

El horario de sondeo está configurado y guardado.

# Instalación de aplicaciones en dispositivos en un entorno de nube

Puede instalar las siguientes aplicaciones de Kaspersky en los dispositivos en un entorno de nube: Kaspersky Security for Windows Server (para dispositivos Windows) y Kaspersky Endpoint Security para Linux (para dispositivos Linux).

Los dispositivos cliente en los cuales tiene la intención de instalar la protección deben cumplir con los requisitos para la operación de Kaspersky Security Center en un entorno de nube. Debe tener una licencia válida para instalar aplicaciones en instancias de AWS, en máquinas virtuales de Microsoft Azure o en instancias de máquinas virtuales de Google.

Kaspersky Security Center 15.1 admite los siguientes escenarios:

- Un dispositivo cliente se descubre mediante una API y la instalación también se realiza mediante una API. Este escenario es compatible con los entornos de nube de AWS y Azure.
- Un dispositivo cliente se descubre mediante sondeo de Active Directory, sondeo de dominios de Windows o sondeo de rango de IP; la instalación se realiza a través de Kaspersky Security Center.
- Un dispositivo cliente se descubre mediante la API de Google y la instalación se realiza mediante Kaspersky Security Center. Para Google Cloud, solo se admite este escenario.

No se admiten otras formas de instalación de las aplicaciones.

Para instalar aplicaciones en dispositivos virtuales, use paquetes de instalación.

*Para crear una tarea de instalación remota de la aplicación en instancias utilizando la API de AWS o la API de Azure:*

1. En el árbol de la consola, seleccione la carpeta **Tareas**.
2. Haga clic en el botón **Nueva tarea**.

   Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente.
3. En la página **Seleccione el tipo de tarea**, seleccione **Instalar aplicación de forma remota** como tipo de la tarea.

4. En la ventana **Seleccionar los dispositivos**, seleccione los dispositivos relevantes desde el grupo **Dispositivos administrados\Nube**.

5. Si el Agente de red todavía no se ha instalado en los dispositivos donde pretende instalar la aplicación, en la página **Seleccione una cuenta para ejecutar la tarea**, seleccione **Se necesita una cuenta (no se utiliza el Agente de red)** y haga clic en el botón **Agregar** en la parte derecha de la ventana. En el menú que aparece el escogido de lo siguiente:

   - **Cuenta Cloud**

     Seleccione esta opción si desea instalar aplicaciones en instancias en AWS y tiene una clave de acceso de AWS IAM con los permisos necesarios, pero no tiene una función de IAM. También seleccione esta opción si desea instalar aplicaciones en dispositivos en el entorno de Azure.

     En la ventana que se abre, proporcione a Kaspersky Security Center las credenciales que le otorguen derechos para instalar aplicaciones en los dispositivos pertinentes.

     Seleccione el entorno de nube: AWS o Azure.

     En el campo **Nombre de la cuenta**, introduzca un nombre para estas credenciales. El nombre aparecerá en la lista de cuentas para ejecutar la tarea.

     Si seleccionó AWS, en los campos **Id. de clave de acceso** y **Clave secreta**, introduzca las credenciales para la cuenta de usuario de IAM que tiene los derechos para instalar aplicaciones en los dispositivos especificados.

     Si seleccionó Azure, en los campos **Id. de suscripción de Azure** y **Contraseña de la aplicación de Azure** introduzca las credenciales para la cuenta de Azure que tiene los derechos para instalar aplicaciones en los dispositivos especificados.

     Si especifica credenciales incorrectas, la tarea de instalación remota terminará con un error en los dispositivos para los que está programada.

   - **Cuenta**

     Para instancias que ejecutan Windows, seleccione esta opción si no tiene intenciones de instalar la aplicación utilizando las herramientas de AWS o API de Azure. En este caso, asegúrese de que los dispositivos en su segmento de la nube cumplan con las condiciones necesarias. Kaspersky Security Center instala aplicaciones solo, sin usar a la API de AWS o API de Azure.

     Si especifica datos incorrectos, la tarea de instalación remota terminará con un error en los dispositivos para los que está programada.

   - **Función de IAM**

     Seleccione esta opción si desea instalar aplicaciones en las instancias del entorno de AWS y tiene una función de IAM con los derechos necesarios.

     Si selecciona esta opción, pero no tiene una función de IAM con los derechos necesarios, la tarea de instalación remota terminará con un error en los dispositivos para los que está programada.

   - **Certificado SSH**

Para instancias que ejecutan Linux, seleccione esta opción si no tiene la intención de instalar la aplicación utilizando las herramientas de AWS o API de Azure. En este caso, asegúrese de que los dispositivos en su segmento de la nube cumplan con las condiciones necesarias. Kaspersky Security Center instala aplicaciones solo, sin usar a la API de AWS o API de Azure.

Deberá especificar la clave privada del certificado SSH; para generar esta clave, puede usar la utilidad ssh-keygen. Tenga en cuenta que Kaspersky Security Center espera que la clave privada esté en formato PEM, pero, de manera predeterminada, la utilidad ssh-keygen genera claves SSH en formato OPENSSH. Kaspersky Security Center no admite el formato OPENSSH. Para crear una clave privada en el formato PEM admitido, agregue la opción `-m PEM` en el comando ssh-keygen. Por ejemplo:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<correo electrónico del usuario>"
```

Puede proporcionar credenciales varias haciendo clic en el botón **Agregar** para cada uno nuevo. Si los segmentos de la nube diferentes necesitan credenciales, proporcione las credenciales para todos los segmentos.

Una vez que el Asistente finalice, la tarea para la instalación remota de la aplicación aparece en la lista de tareas en el espacio de trabajo de la carpeta **Tareas**.

En Microsoft Azure, la instalación remota de aplicaciones de seguridad en una máquina virtual puede provocar la eliminación de la extensión de script personalizada instalada en la máquina virtual.

# Visualización de las propiedades de dispositivos de la nube

*Para ver las propiedades de un dispositivo de nube:*

1. En el árbol de la consola, en el nodo **Descubrimiento de dispositivos** → **Nube**, seleccione el subnodo que corresponde al grupo en donde se encuentra la instancia correspondiente.

   Si no conoce el grupo en donde se encuentra el dispositivo virtual correspondiente, use la función de búsqueda:

   a. Haga clic derecho en el nombre del nodo **Dispositivos administrados** → **Nube** y, luego, seleccione **Buscar** en el menú contextual.

   b. En la ventana que se abre, realice la búsqueda.

      Si existe un dispositivo que cumpla con los criterios que configura, se mostrarán el nombre y los detalles en la parte inferior de la ventana.

2. Haga clic en el nombre con el botón derecho del ratón del nodo relevante. En el menú contextual, seleccione **Propiedades**.

   En la ventana que se abre, se mostrarán las propiedades de objeto.

   La sección **Información del sistema** → **Información general del sistema** contiene las propiedades que son específicas para dispositivos en un entorno de nube:

   - **Dispositivo encontrado mediante API** (**AWS**, **Azure** o **Google Cloud**; si el dispositivo no se puede detectar a través de herramientas API, se mostrará el valor **No**).
   - **Región en la nube**.
   - **Nube VPC** (solo para dispositivos AWS y Google Cloud).
   - **Zona de disponibilidad en la nube** (solo para dispositivos AWS y Google Cloud).
   - **Subred de nube**.
   - **Grupo de ubicación en la nube** (esta unidad solo se muestra si la instancia pertenece a un grupo de ubicación; de lo contrario, no se mostrará).

Haga clic en el botón **Exportar a archivo** para exportar esta información a un archivo .csv o .txt.

# Sincronización con la nube

Durante el funcionamiento de Configuración del entorno de nube, se crea la regla llamada Sincronizar con la nube de manera automática. Esta regla permite que usted mueva automáticamente instancias detectados a cada sondeo, desde el grupo **Dispositivos no asignados** o **Dispositivos administrados\Nube** para poner estas instancias a disposición para la administración centralizada. De manera predeterminada, una vez que se crea esta regla, se la deja habilitada. Puede deshabilitar, modificar o aplicar la regla en cualquier momento.

*Para aplicar la regla "Sincronizar con la nube" o modificar sus propiedades:*

1. En el árbol de la consola, haga clic en el nombre con el botón derecho del ratón del nodo **Descubrimiento de dispositivos**.

2. En el menú contextual, seleccione **Propiedades**.

3. En la ventana **Propiedades** que se abre, en el panel **Secciones**, seleccione **Mover dispositivos**.

4. En la lista de reglas de movimiento de dispositivos en el espacio de trabajo, seleccione **Sincronizar con la nube** y haga clic en el botón **Propiedades** en la parte inferior de la ventana.

   Se abre la ventana de propiedades de la regla.

5. Si es necesario, especifique la siguiente configuración en el grupo de configuración de **segmentos de la nube**:

- **El dispositivo se encuentra en un segmento de la nube**

  La regla solo se aplicará a los dispositivos que se encuentren en el segmento de nube seleccionado. De lo contrario, la regla se aplicará a todos los dispositivos que hayan sido detectados.

  Esta opción está seleccionada de forma predeterminada.

  - **Incluir objetos secundarios**

    La regla se aplicará a todos los dispositivos del segmento seleccionado y a todas las subsecciones de nube anidadas. De lo contrario, la regla solo se aplicará a los dispositivos que estén en el segmento raíz.

    Esta opción está seleccionada de forma predeterminada.

  - **Mover dispositivos de objetos anidados a subgrupos correspondientes**

    Si esta opción está habilitada, los dispositivos de los objetos anidados se moverán automáticamente a los subgrupos que se correspondan con su estructura.

    Si esta opción está deshabilitada, los dispositivos de los objetos anidados se moverán automáticamente a la raíz del subgrupo "Cloud" y no habrá más ramificaciones.

    Esta opción está activada de forma predeterminada.

    - **Crear subgrupos correspondientes a contenedores de dispositivos recién detectados**

      Si esta opción está habilitada, cuando la estructura de **Dispositivos administrados\Nube** no tiene subgrupos que coincidan con la sección que contiene el dispositivo, Kaspersky Security Center crea tales subgrupos. Por ejemplo, si se detecta una nueva subred durante el descubrimiento de dispositivos, se creará un nuevo grupo con el mismo nombre en el grupo **Dispositivos administrados\Cloud**.

      Si esta opción está desactivada, Kaspersky Security Center no crea ningún subgrupo nuevo. Si se descubre una nueva subred al sondear la red, por ejemplo, no se creará un nuevo grupo con el mismo nombre en el grupo **Dispositivos administrados\Cloud**, y los dispositivos que se encuentren en la subred detectada se moverán al grupo **Dispositivos administrados\Cloud**.

      Esta opción está activada de forma predeterminada.

    - **Eliminar subgrupos para los que no se encuentra coincidencia en los segmentos de la nube**

      Si esta opción está habilitada, la aplicación eliminará del grupo "Cloud" todo subgrupo que no tenga contraparte en un objeto de nube existente.

      Si esta opción está deshabilitada, se conservarán los subgrupos que no tengan contraparte en un objeto de nube existente.

      Esta opción está activada de forma predeterminada.

  Si ha activado la opción **Sincronizar con la nube** al ejecutar la Configuración del entorno de nube, se crea la regla Sincronizar con la nube con las casillas **Crear subgrupos correspondientes a contenedores de dispositivos recién detectados** y **Eliminar subgrupos para los que no se encuentra coincidencia en los segmentos de la nube** marcadas.

Si no activó la opción **Sincronizar con la nube**, la regla Sincronizar con la nube se crea con estas opciones desactivadas (eliminadas). Si su trabajo con Kaspersky Security Center requiere que la estructura de los subgrupos en el subgrupo **Dispositivos administrados\Nube** coincida con la estructura de segmentos de la nube, active las opciones **Crear subgrupos correspondientes a contenedores de dispositivos recién detectados** y **Eliminar subgrupos para los que no se encuentra coincidencia en los segmentos de la nube** en las propiedades de la regla y, a continuación, aplique la regla.

6. En la lista desplegable **Dispositivo encontrado mediante API**, seleccione uno de los siguientes valores:
   - **AWS**. El dispositivo se descubre mediante la API de AWS, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de AWS.
   - **Azure**. El dispositivo se descubre mediante la API de Azure, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de Azure.
   - **Google Cloud.** El dispositivo se descubre utilizando la API de Google, es decir, el dispositivo está en el entorno de Google Cloud.
   - **No**. El dispositivo no se puede detectar con la API de AWS, Azure o Google (o bien el dispositivo no se encuentra en el entorno de nube, o bien sí está en el entorno de nube, pero, por algún motivo, no se lo puede detectar con una API).
7. **Ningún valor.** Esta condición no se aplica. Si es necesario, configure otras propiedades de reglas en otras secciones.
8. Si es necesario, aplique la regla haciendo clic en el botón **Forzar** en la parte inferior de la ventana.

   Se inicia el Asistente de ejecución de reglas. Siga las instrucciones del asistente. Cuando el Asistente finaliza, la regla se ejecutará y la estructura de subgrupos en el subgrupo **Dispositivos administrados\Nube** coincidirá con la estructura de sus segmentos de la nube.
9. Haga clic en el botón **Aceptar**.

Las propiedades están configuradas y guardadas.

*Para deshabilitar la regla Sincronizar con Cloud, realice lo siguiente:*

1. En el árbol de la consola, haga clic en el nombre con el botón derecho del ratón del nodo **Descubrimiento de dispositivos**.
2. En el menú contextual, seleccione **Propiedades**.
3. En la ventana **Propiedades** que se abre, en el panel **Secciones**, seleccione **Mover dispositivos**.
4. En la lista de reglas de movimiento de dispositivos en el espacio de trabajo, desactive (elimine) la opción **Sincronizar con la nube** y haga clic en **Aceptar**.

La regla está desactivada y ya no se aplicará.

# Despliegue de Kaspersky Security Center en Yandex.Cloud

Puede desplegar Kaspersky Security Center en Yandex.Cloud. Solo está disponible el modo de pago por uso; las bases de datos en la nube no son compatibles.

En Yandex.Cloud, están disponibles los siguientes métodos de despliegue para las aplicaciones de seguridad:

- Por medio nativo de Kaspersky Security Center, es decir, a través de la tarea *Instalación remota* (el despliegue de los programas de seguridad solo es posible si el Servidor de administración y las máquinas virtuales que se deben proteger están en el mismo segmento de red)
- A través de scripts de despliegue

Para el despliegue de Kaspersky Security Center en Yandex.Cloud, debe tener una cuenta de servicio en Yandex.Cloud. Debe otorgar a esta cuenta el permiso marketplace.meteringAgent y asociarla con la máquina virtual (consulte https://cloud.yandex.com/en para obtener más detalles).

# Apéndices

Esta sección proporciona información de referencia y hechos adicionales sobre el uso de Kaspersky Security Center.

# Características avanzadas

En esta sección se describe una variedad de opciones adicionales de Kaspersky Security Center diseñadas para expandir la funcionalidad de la administración centralizada de aplicaciones en dispositivos.

## Automatización del funcionamiento de Kaspersky Security Center. Utilidad klakaut

Puede automatizar el funcionamiento de Kaspersky Security Center usando la utilidad klakaut. La utilidad klakaut y un sistema de ayuda para ello se encuentran en la carpeta de instalación de Kaspersky Security Center.

## Herramientas personalizadas

Kaspersky Security Center le permite crear una lista de *herramientas personalizadas* (en adelante también denominadas, simplemente, *herramientas*); es decir, aplicaciones activadas para un dispositivo cliente en la Consola de administración mediante el grupo **Herramientas personalizadas** del menú contextual. Cada herramienta de la lista será asociada con un comando de menú independiente, que la Consola de administración utiliza para iniciar la aplicación correspondiente a esa herramienta.

La aplicación se inicia en la estación de trabajo del administrador. La aplicación puede aceptar los atributos de un dispositivo cliente remoto como argumentos de la línea de comandos (nombre NetBIOS, nombre DNS o dirección IP). La conexión con el dispositivo remoto se puede establecer mediante la conexión de túnel.

La lista de herramientas personalizadas contiene los siguientes programas de servicio para cada dispositivo cliente:

- **Diagnóstico remoto** es una utilidad para el diagnóstico remoto de Kaspersky Security Center.
- **Escritorio remoto** es un componente estándar de Microsoft Windows denominado Conexión a Escritorio remoto.
- **Administración de equipos** es un componente estándar de Microsoft Windows.

*Para agregar o eliminar herramientas personalizadas o para editar su configuración,*

En el menú contextual del dispositivo cliente, seleccione **Herramientas personalizadas → Configurar herramientas personalizadas**.

Se abre la ventana **Herramientas personalizadas**. En esta ventana, puede agregar herramientas personalizadas o editar su configuración usando los botones **Agregar** y **Modificar**. Para eliminar una herramienta personalizada, haga clic en el botón Eliminar con el ícono de la cruz roja ( ❌ ).

# Modo de clonación de disco del Agente de red

La clonación del disco duro de un dispositivo de referencia es un método muy utilizado para instalar software en dispositivos nuevos. Si el Agente de red se está ejecutando en modo estándar en el disco duro del dispositivo de referencia, se presenta el siguiente problema:

Una vez que la imagen de referencia con el Agente de red se instala en los dispositivos nuevos, estos aparecen en la Consola de administración bajo un solo icono. El problema se produce porque, debido a la clonación, los datos internos de los dispositivos, que el Servidor de administración utiliza para asociar un dispositivo con un icono en la Consola de administración, son idénticos.

El *modo de clonación de disco del Agente de red* especial le permite evitar la visualización incorrecta de dispositivos nuevos en la Consola de administración luego de la clonación. Use este modo cuando desee realizar un despliegue de software (con el Agente de red) en dispositivos nuevos mediante la clonación de disco.

En el modo de clonación de disco, el Agente de red sigue ejecutándose pero no se conecta al Servidor de administración. Al salir del modo de clonación, el Agente de red elimina los datos internos que hacen que el Servidor de administración asocie varios dispositivos con un solo icono en la Consola de administración. Después de completar la clonación de la imagen del dispositivo de referencia, los dispositivos nuevos se muestran en la Consola de administración correctamente (con iconos individuales).

## Escenario de uso del modo de clonación de disco del Agente de red

1. El administrador instala el Agente de red en un dispositivo de referencia.
2. El administrador comprueba la conexión del Agente de red con el Servidor de administración usando la utilidad klnagchk.
3. El administrador habilita el modo de clonación de disco del Agente de red.
4. El administrador instala software y parches en el dispositivo, y lo reinicia tantas veces como sea necesario.

5. El administrador clona el disco duro del dispositivo de referencia en cuantos dispositivos sea necesario.
6. Cada copia clonada debe cumplir las siguientes condiciones:
    a. Se debe cambiar el nombre del dispositivo.
    b. Se debe reiniciar el dispositivo.
    c. Se debe deshabilitar el modo de clonación de disco.

### Habilitación y deshabilitación del modo de clonación de disco mediante la utilidad klmover

*Para activar o desactivar el modo de clonación de disco del Agente de red:*

1. Ejecute la utilidad klmover en el dispositivo con el Agente de red instalado que necesita clonar.
   La utilidad klmover se encuentra en la carpeta de instalación del Agente de red.
2. Para habilitar el modo de clonación de disco, ingrese el siguiente comando en el símbolo del sistema de Windows:
   `klmover -cloningmode 1`
   El Agente de red cambia al modo de clonación de disco.
3. Para solicitar el estado actual del modo de clonación de disco, ingrese el siguiente comando en el símbolo del sistema:
   `klmover -cloningmode`
   La ventana de la utilidad indica si el modo de clonación de disco está habilitado o no.
4. Para deshabilitar el modo de clonación de disco, ingrese el siguiente comando en la línea de comandos de la utilidad:
   `klmover -cloningmode 0`

## Preparación de un dispositivo de referencia con el Agente de red instalado para crear una imagen del sistema operativo

Es posible que desee crear una imagen del sistema operativo de un dispositivo de referencia con el Agente de red instalado y luego instalar esa imagen en los dispositivos de la red. En este caso, crea una imagen del sistema operativo de un dispositivo de referencia en el que el Agente de red aún no se ha iniciado. Si inicia el Agente de red en un dispositivo de referencia antes de crear una imagen del sistema operativo, la identificación del Servidor de administración de los dispositivos en los que se instale la imagen del sistema operativo del dispositivo de referencia será problemática.

*Para preparar el dispositivo de referencia para crear una imagen del sistema operativo:*

1. Asegúrese de que el sistema operativo Windows esté instalado en el dispositivo de referencia e instale el otro software que necesita en ese dispositivo.
2. En el dispositivo de referencia, en la configuración de Conexiones de red de Windows, desconecte el dispositivo de referencia de la red donde está instalado Kaspersky Security Center.

3. En el dispositivo de referencia, inicie la instalación local del Agente de red utilizando el archivo setup.exe.

   Se inicia el Asistente de instalación del Agente de red de Kaspersky Security Center. Siga las instrucciones del asistente.

4. En la página **Servidor de administración** del asistente, especifique la dirección IP del Servidor de administración.

   Si no conoce la dirección exacta del Servidor de administración, introduzca localhost. Puede cambiar la dirección IP más tarde utilizando la utilidad klmover con la clave `-address`.

5. En la página de **inicio de la aplicación** del asistente, deshabilite la opción **Iniciar la aplicación durante la instalación**.

6. Cuando finalice la instalación del Agente de red, no reinicie el dispositivo antes de crear una imagen del sistema operativo.

   Si reinicia el dispositivo, deberá repetir todo el proceso de preparación de un dispositivo de referencia para crear una imagen del sistema operativo.

7. En el dispositivo de referencia, en la línea de comando, inicie la utilidad sysprep y ejecute el siguiente comando: `sysprep.exe /generalize /oobe /shutdown`.

El dispositivo de referencia está listo para crear una imagen del sistema operativo.

## Configuración de la recepción de mensajes del Monitor de integridad de archivos

Ciertas aplicaciones administradas, como Kaspersky Security for Windows Server y Kaspersky Security for Virtualization Light Agent, envían mensajes del Monitor de integridad de archivos a Kaspersky Security Center. Kaspersky Security Center también le permite supervisar cualquier cambio en los componentes importantes de los sistemas (por ejemplo, servidores web y cajeros automáticos) y responder lo antes posible a incumplimientos de la integridad de tales sistemas. Para tal fin, puede recibir los mensajes del componente Monitor de integridad de archivos. Este componente puede usarse para supervisar no solo el sistema de archivos de un dispositivo, sino también las subramas del Registro, el estado del firewall y el estado del hardware conectado.

Kaspersky Security Center debe configurarse para recibir los mensajes del Monitor de integridad de archivos sin usar Kaspersky Security for Windows Server o Kaspersky Security for Virtualization Light Agent.

*Para configurar la recepción de mensajes del Monitor de integridad de archivos:*

1. Abra el registro del sistema del dispositivo en el que está instalado el Servidor de administración (por ejemplo, de forma local con el comando regedit en el menú **Iniciar** → **Ejecutar**).

2. Vaya al siguiente archivo:

   - Para sistemas de 32 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

   - Para sistemas de 64 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF

3. Crear claves:

   - Cree la clave KLSRV_EVP_FIM_PERIOD_SEC para especificar el período de tiempo para contar el número de eventos procesados. Configure los siguientes ajustes:

     a. Especifique KLSRV_EVP_FIM_PERIOD_SEC como nombre de la clave.

     b. Especifique DWORD como tipo de clave.

     c. Especifique un intervalo de valores para el intervalo de tiempo desde 43 200 hasta 172 800 segundos. De forma predeterminada, el intervalo de tiempo es 86 400 segundos.

   - Cree la clave KLSRV_EVP_FIM_LIMIT para limitar el número de eventos recibidos para el intervalo de tiempo especificado. Configure los siguientes ajustes:

     a. Especifique KLSRV_EVP_FIM_LIMIT como nombre de clave.

     b. Especifique DWORD como tipo de clave.

     c. Especifique un intervalo de valores para eventos recibidos desde 2 000 hasta 50 000. El número predeterminado de eventos es de 20 000.

   - Cree la clave KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC para contar eventos con exactitud hasta un intervalo de tiempo específico. Configure los siguientes ajustes:

     a. Especifique KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC como nombre de clave.

     b. Especifique DWORD como tipo de clave.

     c. Especifique un rango de valores de 120 a 600 segundos. De forma predeterminada, el intervalo de tiempo es 300 segundos.

   - Cree la clave KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC de modo que, después de la cantidad de tiempo especificada, la aplicación pueda comprobar si el número de eventos procesados a lo largo del intervalo de tiempo está siendo inferior al límite especificado. Esta verificación se realiza al alcanzar el límite de eventos que se pueden recibir. Si esta condición se cumple, la aplicación reanuda el almacenamiento de eventos en la base de datos. Configure los siguientes ajustes:

     a. Especifique KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC como nombre de clave.

     b. Especifique DWORD como tipo de clave.

     c. Especifique un intervalo de valores desde 600 hasta 3 600 segundos. De forma predeterminada, el intervalo de tiempo es 1 800 segundos.

   Si las claves no se crean, los valores predeterminados se utilizan.

4. Reinicie el servicio del Servidor de administración.

Se configurarán los límites de la recepción de eventos del componente Monitor de integridad de archivos. Puede ver los resultados del componente Monitor de integridad de archivos en los informes denominados **Las 10 reglas Monitor de integridad de archivos / Control de integridad del sistema que se activaron con mayor frecuencia en los dispositivos** y **Los 10 dispositivos cuyas reglas de Monitor de integridad de archivos / Control de integridad del sistema se desencadenan con mayor frecuencia**.

# Mantenimiento del Servidor de administración

El mantenimiento del Servidor de administración permite liberar espacio en la carpeta del Servidor de administración y reducir el volumen de las bases de datos al eliminar objetos que ya no son necesarios. Esto lo ayuda a mejorar el rendimiento y la fiabilidad operativa de la aplicación. Recomendamos que realice el mantenimiento del Servidor de administración al menos una vez a la semana.

El mantenimiento del Servidor de administración se lleva a cabo a través de la tarea especializada. La aplicación realiza las acciones siguientes durante el mantenimiento del Servidor de administración:

- Elimina carpetas y archivos innecesarios de la carpeta de almacenamiento.
- Elimina los registros innecesarios de las tablas (también conocidos como "referencias colgantes").
- Borra la caché.
- Mantiene las bases de datos (si usa SQL Server o PostgreSQL como DBMS):
  - Comprueba las bases de datos en busca de errores (disponible solo para SQL Server).
  - Reorganiza los índices de la base de datos.
  - Actualiza las estadísticas de la base de datos.
  - Reduce la base de datos si es necesario.

*Para crear la tarea Mantenimiento del Servidor de administración, siga estos pasos:*

1. En el árbol de consola, seleccione el nodo del Servidor de administración para el que desee crear la tarea *Mantenimiento del Servidor de administración*.
2. Seleccione la carpeta **Tareas**.
3. En el espacio de trabajo de la carpeta **Tareas**, haga clic en el botón **Nueva tarea**.

   Se inicia el Asistente para crear nueva tarea.
4. En la ventana del Asistente **Seleccione el tipo de tarea**, seleccione **Mantenimiento del Servidor de administración** como tipo de tarea y luego haga clic en **Siguiente**.
5. Si necesita reducir la base de datos del Servidor de administración durante el mantenimiento, en la ventana **Configuración** del Asistente, seleccione la casilla de verificación **Reducir la base de datos**.
6. Siga el resto de instrucciones del asistente.

La tarea nueva se muestra en la lista de tareas del espacio de trabajo de la carpeta **Tareas**. Solo puede haber una tarea *Mantenimiento del Servidor de administración* en ejecución por cada Servidor de administración. Si creó creado una tarea *Mantenimiento del Servidor de administración* para un Servidor de administración, no podrá crear una nueva tarea *Mantenimiento del Servidor de administración*.

## Acceso a los servidores DNS públicos

Si no es posible acceder a los servidores de Kaspersky mediante los servidores DNS del sistema, Kaspersky Security Center puede utilizar los siguientes servidores DNS públicos en el siguiente orden:

1. Servidores DNS públicos de Google (8.8.8.8)
2. Servidores DNS de Cloudflare (1.1.1.1)
3. Servidores DNS de Alibaba Cloud (223.6.6.6)
4. Servidores DNS de Quad9 (9.9.9.9)
5. CleanBrowsing (185.228.168.168)

Las solicitudes realizadas a estos servidores DNS pueden contener direcciones de dominio y la dirección IP pública del Servidor de administración, ya que la aplicación establece una conexión TCP/UDP con los servidores DNS. Si Kaspersky Security Center utiliza un servidor DNS público, el procesamiento de datos se rige por la política de privacidad del servicio correspondiente.

*Para configurar el uso de servidores DNS públicos a través de la utilidad klscflag:*

1. Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada es <Disk>:\Archivos de programa(x86)\Kaspersky Lab\Kaspersky Security Center.
2. Para deshabilitar el uso de servidores DNS públicos, ejecute el siguiente comando:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. Para habilitar el uso de servidores DNS públicos, ejecute el siguiente comando:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

## Ventana Método de notificación al usuario

En la ventana **Método de notificación al usuario**, puede configurar la notificación al usuario acerca de la instalación del certificado en el dispositivo móvil:

- **Mostrar código QR en el asistente**. Si selecciona esta opción, se mostrará un enlace al paquete de instalación en el paso final del Asistente para conectar un nuevo dispositivo móvil.
- **Enviar código QR al usuario**. Si selecciona esta opción, podrá especificar la configuración para notificar al usuario sobre la conexión de un dispositivo.

En el grupo de configuración **Por correo electrónico**, puede configurar notificaciones de usuario sobre la instalación de un nuevo certificado en su dispositivo móvil mediante mensajes de correo electrónico. Este método de notificación solo está disponible si el Servidor SMTP está habilitado.

En el grupo de ajustes **Por SMS**, puede configurar la notificación del usuario sobre la instalación de un certificado en su dispositivo móvil mediante SMS. Este método de notificación solo está disponible si Notificación por SMS está habilitada.

Haga clic en el enlace **Editar mensaje** en los grupos de configuración **Por correo electrónico** y **Por SMS** para ver y editar el mensaje de notificación, si fuera necesario.

## Ventana Selección de dispositivos

Elija una selección de la lista **Selección de dispositivos**. La lista contiene las selecciones predefinidas y las selecciones creadas por el usuario.

Puede ver los detalles de las selecciones de dispositivos en el espacio de trabajo de la sección **Selecciones de dispositivos**.

## Ventana Definir el nombre del nuevo objeto

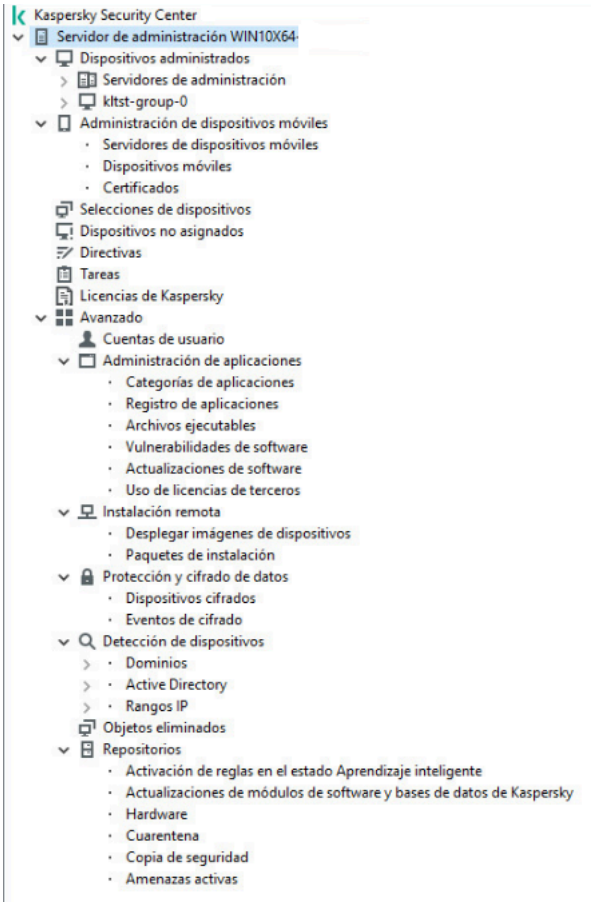
En la ventana, especifique el nombre del objeto recién creado. El nombre no puede tener más de 100 caracteres ni incluir caracteres especiales ("*<>?\:|).

# Características de uso de la interfaz de administración

En esta sección se describen las acciones que se pueden realizar en la ventana principal de Kaspersky Security Center.

# Árbol de consola

El árbol de consola (ver la figura siguiente) está diseñado para mostrar la jerarquía de los Servidores de administración de la red corporativa, la estructura de sus grupos de administración y otros objetos de la aplicación, como las carpetas **Repositorios** o **Administración de aplicaciones**. El espacio de nombres de Kaspersky Security Center puede contener varios nodos incluyendo los nombres de los servidores correspondientes a los Servidores de administración incluidos en la jerarquía.




Árbol de consola

## Nodo Servidor de administración

El nodo **Servidor de administración - <Nombre del dispositivo>** es un contenedor que muestra la organización estructural del Servidor de administración seleccionado.

El espacio de trabajo del nodo **Servidor de administración** contiene información resumida acerca del estado actual de la aplicación y los dispositivos administrados mediante el Servidor de administración. La información del espacio de trabajo se distribuye en varias fichas:

- **Supervisión**. Muestra información acerca del funcionamiento de la aplicación y el estado actual de los dispositivos cliente en tiempo real. Los mensajes importantes para el administrador (como mensajes sobre vulnerabilidades, errores o detecciones de virus) se resaltan con un color específico. Puede usar los vínculos de la ficha **Supervisión** para realizar las tareas estándares de administrador (por ejemplo, instalar y configurar la aplicación de seguridad en dispositivos cliente) y para ir a otras carpetas del árbol de consola.

- **Estadísticas**. Contiene un conjunto de gráficos agrupados por tema (estado de la protección, estadísticas antivirus, actualizaciones, etc.). Estos gráficos muestran información actual sobre el funcionamiento de la aplicación y el estado de los dispositivos cliente.

- **Informes**. Contiene plantillas para informes generadas por la aplicación. En esta ficha, puede crear informes a partir de las plantillas predefinidas y crear plantillas de informes personalizadas.

- Ventana **Eventos**. Contiene registros acerca de los eventos que se registraron durante el funcionamiento de la aplicación. Los registros se organizan por tema para facilitar el filtrado y la lectura. En esta ficha, puede ver las selecciones de eventos que se generaron automáticamente y crear selecciones personalizadas.

## Carpetas en el nodo Servidor de administración

El nodo **Servidor de administración – <Nombre del dispositivo>** incluye las siguientes carpetas:

- **Dispositivos administrados**. La carpeta está diseñada para almacenar, mostrar, configurar y modificar la estructura de los grupos de administración, directivas de grupo y tareas de grupo.

- **Administración de dispositivos móviles**. La carpeta está diseñada para administrar dispositivos móviles. La carpeta **Administración de dispositivos móviles** contiene las siguientes subcarpetas:

  - **Servidores de dispositivos móviles**. Está diseñada para administrar servidores de MDM para iOS.

  - **Dispositivos móviles**. Está diseñada para administrar dispositivos móviles, KES y MDM para iOS.

  - **Certificados**. Está diseñada para administrar certificados de dispositivos móviles.

- **Selecciones de dispositivos**. La carpeta está diseñada para la selección rápida de dispositivos que cumplen los criterios especificados (una selección de dispositivos) entre todos los dispositivos administrados. Por ejemplo, puede seleccionar rápidamente los dispositivos en los que no se ha instalado ninguna aplicación de seguridad y dirigirse a estos dispositivos (ver la lista). Puede realizar algunas acciones específicas en estos dispositivos seleccionados; por ejemplo, asignarles algunas tareas. Puede usar selecciones predefinidas o crear selecciones personalizadas.

- **Dispositivos no asignados**. La carpeta contiene una lista de dispositivos que no se incluyeron en ningún grupo de administración. Puede realizar algunas acciones en los dispositivos no asignados, por ejemplo, moverlos a grupos de administración o instalar aplicaciones.

- **Directivas**. La carpeta está diseñada para ver y crear directivas.

- **Tareas**. La carpeta está diseñada para ver y crear tareas.

- **Licencias de Kaspersky**. Contiene una lista de las claves de licencia disponibles para las aplicaciones de Kaspersky. En el espacio de trabajo de esta carpeta, puede agregar claves de licencia nuevas al repositorio de claves de licencia, distribuir claves de licencia a dispositivos administrados y ver informes sobre el uso de claves de licencia.

- **Avanzado**. La carpeta contiene un conjunto de subcarpetas que corresponden a varios grupos de las características de la aplicación.

## Carpeta Avanzado. Mover carpetas en el árbol de consola

La carpeta **Avanzado** incluye las siguientes subcarpetas:

- **Cuentas de usuario**. Contiene una lista de las cuentas de usuarios de la red.
- **Administración de aplicaciones**. Diseñada para administrar las aplicaciones instaladas en los dispositivos de la red. La carpeta **Administración de aplicaciones** contiene las siguientes subcarpetas:
  - **Categorías de aplicaciones**. Diseñado para administrar categorías de aplicaciones personalizadas.
  - **Registro de aplicaciones**. Contiene una lista de aplicaciones en dispositivos cliente en los que se encuentra instalado el Agente de red.
  - **Archivos ejecutables**. Contiene la lista de archivos ejecutables almacenados en dispositivos cliente en los que se encuentra instalado el Agente de red.
  - **Vulnerabilidades de software**. Contiene la lista de vulnerabilidades de aplicaciones de dispositivos en los que se encuentra instalado el Agente de red.
  - **Actualizaciones de software**. Contiene una lista de actualizaciones de la aplicación recibidas por el Servidor de administración que se pueden distribuir a los dispositivos.
  - **Uso de licencias de terceros**. Contiene una lista de grupos de aplicaciones con licencia. Puede usar grupos de aplicaciones con licencia para supervisar el uso de licencias de software de terceros (aplicaciones ajenas a Kaspersky) y posibles violaciones de los límites de la licencia.
- **Instalación remota**. La carpeta está diseñada para administrar la instalación remota de sistemas operativos y aplicaciones. La carpeta **Instalación remota** contiene las siguientes subcarpetas:
  - **Desplegar imágenes de dispositivos**. Está diseñada para distribuir imágenes de sistemas operativos en dispositivos.
  - **Paquetes de instalación**. Contiene una lista de los paquetes de instalación que se pueden utilizar para la instalación remota de aplicaciones en dispositivos.
- **Protección y cifrado de datos**. Desde aquí puede gestionarse el proceso de cifrado de datos en discos duros y unidades extraíbles.

- **Sondeo de red**. La carpeta muestra la red donde se encuentra instalado el Servidor de administración. El Servidor de administración recopila información sobre la estructura de la red y sus dispositivos mediante sondeos regulares de la red Windows, las subredes IP y Active Directory® en la red corporativa. Los resultados de sondeo se muestran en los espacios de trabajo de las carpetas correspondientes: **Dominios**, **Rangos IP** y **Active Directory**.

- **Repositorios**. La carpeta está diseñada para las operaciones con objetos utilizados para supervisar el estado de los dispositivos y llevar a cabo su mantenimiento. La carpeta **Repositorios** contiene las siguientes subcarpetas:

  - **Detección adaptable de anomalías**. Contiene una lista de detecciones realizada mediante las reglas de Kaspersky Endpoint Security que funcionan en el modo Aprendizaje inteligente en los dispositivos cliente.

  - **Parches y actualizaciones de software de Kaspersky**. Contiene una lista de actualizaciones recibidas por el Servidor de administración que se pueden distribuir a los dispositivos.

  - **Hardware**. Contiene una lista del hardware conectado a la red de la organización.

  - **Cuarentena**. Contiene una lista de objetos colocados en Cuarentena por las aplicaciones antivirus en dispositivos.

  - **Copias de seguridad**. Contiene una lista de copias de seguridad de los archivos que se eliminaron o modificaron durante la desinfección en dispositivos.

  - **Archivos no procesados**. Contiene una lista de los archivos asignados para escaneo posterior por las aplicaciones antivirus.

Puede cambiar el conjunto de subcarpetas que se incluyen en la carpeta **Avanzado**. Las subcarpetas con frecuencia usadas se pueden subir un nivel desde la carpeta **Avanzado**. Las subcarpetas que se usan con poca frecuencia se pueden mover a la carpeta **Avanzado**.

*Para mover una subcarpeta de la carpeta **Avanzado**:*

1. En el árbol de consola, seleccione la subcarpeta que desea mover de la carpeta **Avanzado**.
2. En el menú contextual de la subcarpeta, seleccione **Ver** → **Mover de la carpeta Avanzado**.

> También puede mover una subcarpeta de la carpeta **Avanzado** desde el espacio de trabajo de la carpeta **Avanzado** haciendo clic en el vínculo **Mover de la carpeta Avanzado** que se encuentra en la sección con el nombre de la subcarpeta.

*Para mover una subcarpeta a la carpeta **Avanzado**:*

1. En el árbol de consola, seleccione la subcarpeta que desea mover a la carpeta **Avanzado**.
2. En el menú contextual de la subcarpeta, seleccione **Ver** → **Mover a la carpeta Avanzado**.

## Cómo actualizar datos en el espacio de trabajo

> En Kaspersky Security Center, los datos del espacio de trabajo (por ejemplo, estados del dispositivo, estadísticas e informes) nunca se actualizan automáticamente.

*Para actualizar los datos en el espacio de trabajo:*

- Presione la tecla **F5**.
- En el menú contextual del objeto en el árbol de consola, seleccione **Actualizar**.
- Haga clic en el ícono de actualización (  ) en el espacio de trabajo.

## Cómo navegar en el árbol de consola

Para desplazarse por el árbol de consola, puede utilizar los siguientes botones de la barra de herramientas:

-  : Un paso hacia atrás.
-  : Un paso hacia adelante.
-  : Un nivel hacia arriba.

También puede utilizar una cadena de navegación ubicada en la esquina superior derecha del espacio de trabajo. La cadena de navegación le indicará la ruta completa a la carpeta del árbol de consola en la que se encuentre en ese momento. Todos los elementos de la cadena, excepto el último, son enlaces a los objetos en el árbol de consola.

## Cómo abrir la ventana de propiedades de un objeto en el espacio de trabajo

Puede cambiar las propiedades de la mayor parte de los objetos de la Consola de administración en la ventana de propiedades del objeto.

*Para abrir la ventana de propiedades de un objeto ubicado en el espacio de trabajo:*

- En el menú contextual del objeto, seleccione **Propiedades**.
- Seleccione un objeto y presione **ALT+INTRO**.

## Cómo seleccionar un grupo de objetos en el espacio de trabajo

Puede seleccionar un grupo de objetos en el espacio de trabajo. Puede seleccionar un grupo de objetos, por ejemplo, para crear un conjunto de dispositivos para los cuales puede crear tareas más adelante.

*Para seleccionar un intervalo de objetos:*

1. Seleccione el primer objeto en el intervalo y presione **Mayús**.
2. Mantenga presionada la tecla **Mayús** y seleccione el último objeto del intervalo.

El intervalo quedará seleccionado.

*Para agrupar objetos separados:*

1. Seleccione el primer objeto del grupo y presione **Ctrl**.
2. Mantenga presionada la tecla **Ctrl** y seleccione los demás objetos que desea incluir en el grupo.

Los objetos serán agrupados.

## Cómo cambiar el conjunto de columnas en el espacio de trabajo

La Consola de administración permite cambiar un conjunto de columnas que se muestran en el espacio de trabajo.

*Para cambiar el conjunto de columnas que se muestran en el espacio de trabajo:*

1. En el árbol de consola, haga clic en el objeto para el cual desea cambiar el conjunto de columnas.
2. En el espacio de trabajo de la carpeta, abra la ventana requerida para la configuración del conjunto de columnas haciendo clic en el enlace **Agregar/eliminar columnas**.
3. En la ventana **Agregar/eliminar columnas**, especifique el conjunto de columnas para mostrar.

# Información de referencia

En las tablas de esta sección se proporciona información de resumen acerca del menú contextual de los objetos de la Consola de administración, así como información sobre los estados de los objetos del árbol de consola y los objetos del espacio de trabajo.

## Comandos del menú contextual

En esta sección, se enumeran los objetos de la Consola de administración y los elementos correspondientes del menú contextual (vea la tabla a continuación).

Elementos del menú contextual de los objetos de la Consola de administración

| Objeto | Elemento del menú | Finalidad del elemento del menú |
|---|---|---|
| Elementos generales del menú contextual | **Buscar** | Abrir la ventana de búsqueda de dispositivos. |
| | **Actualizar** | Actualizar la visualización del objeto seleccionado. |
| | **Exportar lista** | Exportar la lista actual a un archivo. |
| | **Propiedades** | Abrir la ventana de propiedades del objeto seleccionado. |
| | **Ver → Agregar/eliminar columnas** | Agregar o eliminar columnas en la tabla de objetos del espacio de trabajo. |
| | **Ver → Íconos grandes** | Mostrar los objetos del espacio de trabajo en forma de iconos grandes. |
| | **Ver → Íconos pequeños** | Mostrar los objetos del espacio de trabajo en forma de iconos pequeños. |
| | **Ver → Lista** | Mostrar los objetos del espacio de trabajo en forma de lista. |
| | **Ver → Tabla** | Mostrar los objetos del espacio de trabajo en forma de tabla. |
| | **Ver → Configurar** | Configurar la visualización de elementos de la Consola de administración. |
| **Kaspersky Security Center** | **Nuevo → Servidor de administración** | Agregar un Servidor de administración al árbol de la consola. |
| **<Nombre del Servidor de administración>** | **Conectarse al Servidor de administración** | Establecer conexión con el Servidor de administración. |
| | **Desconectarse del Servidor de administración** | Desconectarse del Servidor de administración. |
| **Dispositivos administrados** | **Instalar aplicación** | Iniciar el Asistente de instalación remota. |
| | **Ver → Configuración de interfaz** | Configurar la visualización de elementos de la interfaz. |
| | **Eliminar** | Eliminar un Servidor de administración del árbol de la consola. |
| | **Instalar aplicación** | Iniciar el Asistente de instalación remota para el grupo de administración. |
| | **Restablecer contador de virus** | Restablecer los contadores de virus para los dispositivos incluidos en el grupo de administración. |
| | **Ver informe de amenazas** | Crear un informe sobre las amenazas y la actividad viral registradas en los dispositivos del grupo de administración. |
| | **Nuevo → Grupo** | Crear un grupo de administración. |
| | **Todas las tareas → Nueva estructura de grupo** | Crear una estructura de grupos de administración basada en la estructura de dominios o en la estructura de Active Directory. |
| | **All Tasks → Mostrar mensaje** | Iniciar el "Asistente de nuevo mensaje para usuario" para los usuarios de los dispositivos cliente incluidos en el grupo de administración. |
| **Dispositivos administrados → Servidores de administración** | **New → Servidor de administración secundario** | Iniciar el Asistente para agregar un Servidor de administración secundario. |
| | **New → Servidor de administración virtual** | Iniciar el Asistente para crear un Servidor de administración virtual. |
| **Administración de dispositivos móviles → Dispositivos móviles** | **Nuevo → Dispositivo móvil** | Conectar un nuevo dispositivo móvil perteneciente al usuario. |
| **Administración de dispositivos móviles → Certificados** | **Nuevo → Certificado** | Crear un certificado. |
| | **Crear → Dispositivo móvil** | Conectar un nuevo dispositivo móvil perteneciente al usuario. |

| Objeto | Elemento del menú | Finalidad del elemento del menú |
|---|---|---|
| **Selecciones de dispositivos** | **Nuevo → Nueva selección** | Crear una selección de dispositivos. |
| | **Todas las tareas → Importar** | Importar una selección desde un archivo. |
| **Licencias de Kaspersky** | **Agregar código de activación o archivo de clave** | Agregar una clave de licencia al repositorio del Servidor de administración. |
| | **Activar aplicación** | Iniciar el Asistente para la creación de tareas de activación de aplicaciones. |
| | **Informe de uso de claves de licencia** | Crear y mostrar un informe sobre las claves de licencia utilizadas en los dispositivos cliente. |
| **Administración de aplicaciones → Categorías de aplicaciones** | **Nuevo → Categoría** | Crear una categoría de aplicaciones. |
| **Administración de aplicaciones → Registro de aplicaciones** | **Filtro** | Configurar un filtro para la lista de aplicaciones. |
| | **Aplicaciones supervisadas** | Configurar la publicación de eventos relacionados con la instalación de aplicaciones. |
| | **Eliminar aplicaciones que no están instaladas** | Quitar de la lista los detalles de las aplicaciones que ya no estén instaladas en los dispositivos conectados a la red. |
| **Administración de aplicaciones → Actualizaciones de software** | **Aceptar Contratos de licencia de las actualizaciones** | Aceptar los contratos de licencia de las actualizaciones de software. |
| **Administración de aplicaciones → Uso de licencias de terceros** | **Nuevo → Grupo de aplicaciones con licencia** | Crear un grupo de aplicaciones con licencia. |
| **Instalación remota → Paquetes de instalación** | **Mostrar las versiones actuales de las aplicaciones** | Mostrar una lista con las últimas versiones disponibles en los servidores web para las aplicaciones de Kaspersky. |
| | **Nuevo → Paquete de instalación** | Crear un paquete de instalación. |
| | **All Tasks → Actualizar bases de datos** | Actualizar las bases de datos de una aplicación en los paquetes de instalación correspondientes. |
| | **Todas las tareas → Mostrar la lista general de paquetes independientes** | Mostrar la lista de paquetes independientes creados para los paquetes de instalación. |
| **Descubrimiento de dispositivos → Dominios** | **Todas las tareas → Actividad de los dispositivos** | Definir cómo responderá el Servidor de administración a la inactividad de los dispositivos conectados a la red. |
| **Descubrimiento de dispositivos → Intervalos IP** | **Nuevo → Intervalo IP** | Crear un intervalo IP. |
| **Repositorios → Actualizaciones para bases de datos y módulos de software de Kaspersky** | **Descargar actualizaciones** | Abrir la ventana de propiedades de la tarea del Servidor de administración "Descargar actualizaciones en el repositorio". |
| | **Configuración de descarga de actualizaciones** | Configurar la tarea del Servidor de administración "Descargar actualizaciones en el repositorio". |
| | **Informe de uso de las bases de datos antivirus** | Crear y mostrar un informe sobre las versiones de las bases de datos. |
| | **All Tasks → Eliminar el repositorio de actualizaciones** | Vaciar el repositorio de actualizaciones del Servidor de administración. |
| **Repositorios → Hardware** | **Nuevo → Dispositivo** | Crear un nuevo dispositivo. |

## Lista de dispositivos administrados. Descripción de las columnas

La siguiente tabla muestra los nombres y las descripciones de las columnas que conforman la lista de dispositivos administrados.

Descripciones de las columnas de la lista de dispositivos administrados

| Nombre de la columna | Valor |
|---|---|
| Nombre | Nombre NetBIOS del dispositivo cliente. Las descripciones de los iconos de los nombres de dispositivos se encuentran en el apéndice. |
| Tipo de sistema operativo | El tipo de sistema operativo instalado en el dispositivo cliente. |
| Dominio de Windows | El nombre del dominio de Windows en el que está ubicado el dispositivo cliente. |
| Agente de red instalado | El resultado de la instalación del Agente de red en el dispositivo cliente: *Sí*, *No*, *Desconocido*. |
| Agente de red en ejecución | El resultado de la puesta en funcionamiento del Agente de red: *Sí*, *No*, *Desconocido*. |
| Protección en tiempo real | Indicación de si la aplicación de seguridad está instalada *Sí*, *No*, *Desconocido*. |
| Última conexión con el Servidor de administración | El tiempo transcurrido desde que el dispositivo cliente se conectó al Servidor de administración. |
| Última actualización de las bases de datos antivirus | El tiempo transcurrido desde que los dispositivos cliente se actualizaron por última vez. |
| Estado | El estado actual del dispositivo cliente: *Sin inconvenientes, Crítico o Advertencia*. |

| Nombre de la columna | Valor |
| --- | --- |
| Descripción del estado | Las condiciones por las que el estado del dispositivo cliente cambió a *Crítico* o *Advertencia*.<br>El estado de un dispositivo puede cambiar a *Crítico* o *Advertencia* por las siguientes circunstancias:<br>• La aplicación de seguridad no está instalada.<br>• Se detectaron demasiados virus.<br>• El nivel de protección en tiempo real difiere del nivel establecido por el administrador.<br>• No se ha realizado un análisis antimalware en mucho tiempo.<br>• Las bases de datos están desactualizadas.<br>• Sin conexión desde hace mucho tiempo.<br>• Se han detectado amenazas activas.<br>• Se debe reiniciar el dispositivo.<br>El motivo para reiniciar el dispositivo puede ser uno de los siguientes:<br>◦ Reiniciado por motivo desconocido.<br>◦ La aplicación no se ejecutará hasta que se reinicie el equipo.<br>◦ Se debe reiniciar el dispositivo para completar la actualización que está ejecutando la aplicación.<br>◦ Se requiere reiniciar para iniciar la actualización.<br>◦ Se debe reiniciar el dispositivo para completar el análisis o la desinfección.<br>◦ Se requiere reiniciar para completar la instalación o la desinstalación remotas.<br>◦ Completando cifrado de datos en disco.<br>Puede establecer los motivos al configurar el cambio de estados del dispositivo.<br>• Hay aplicaciones incompatibles instaladas.<br>• Se detectaron vulnerabilidades de software.<br>• La búsqueda de actualizaciones de Windows Update no se ha realizado en mucho tiempo.<br>• Estado de cifrado no válido.<br>• La configuración del dispositivo móvil no cumple con la directiva.<br>• Problemas de seguridad no procesados detectados.<br>• Estado del dispositivo definido por la aplicación.<br>• El dispositivo no tiene espacio en el disco.<br>• La licencia está por caducar.<br>El estado de un dispositivo puede cambiar a *Crítico* únicamente por los siguientes motivos:<br>• La licencia caducó.<br>• El dispositivo ha cambiado a no administrado.<br>• Protección deshabilitada.<br>• La aplicación de seguridad no está en ejecución.<br>Las aplicaciones de Kaspersky administradas de los dispositivos cliente pueden agregar descripciones de estado a la lista. Kaspersky Security Center puede recibir una descripción del estado de un dispositivo cliente a través de las aplicaciones administradas de Kaspersky instaladas en ese dispositivo. Si el estado asignado al dispositivo a través de la aplicación administrada es diferente del asignado por Kaspersky Security Center, la Consola de administración muestra el estado más crítico para la seguridad del dispositivo. Por ejemplo, si la aplicación administrada asigna el estado *Crítico* al dispositivo y Kaspersky Security Center le asigna el estado *Advertencia*, la Consola de administración muestra el estado *Crítico* para el dispositivo junto con la descripción correspondiente provista por la aplicación administrada. |
| Información actualizada | El tiempo transcurrido desde que el dispositivo cliente se sincronizó por última vez con el Servidor de administración (es decir, el tiempo transcurrido desde el último sondeo de la red). |
| Nombre DNS | El nombre de dominio DNS del dispositivo cliente. |
| Dominio DNS | El sufijo DNS principal. |
| Dirección IP | La dirección IP del dispositivo cliente. Se recomienda usar la dirección IPv4. |
| Visible por última vez | El periodo de tiempo durante el cual el dispositivo cliente ha estado visible en la red. |
| Último análisis completo | La fecha y hora del último análisis del dispositivo cliente realizado por la aplicación de seguridad a solicitud del usuario. |
| Número total de amenazas detectadas | El número de amenazas encontradas. |

| Nombre de la columna | Valor |
|---|---|
| Estado de la protección en tiempo real | El estado de la protección en tiempo real: *Iniciándose*, *En ejecución*, *En ejecución (protección máxima)*, *En ejecución (velocidad máxima)*, *En ejecución (configuración recomendada)*, *En ejecución (configuración personalizada)*, *Detenido*, *En pausa*, *Error*. |
| Dirección IP de conexión | La dirección IP que se usa para conectarse al Servidor de administración de Kaspersky Security Center. |
| Versión del Agente de red | La versión del Agente de red. |
| Versión de la aplicación | La versión de la aplicación de seguridad instalada en el dispositivo cliente. |
| Base de datos antivirus publicada el | La versión de las bases de datos antivirus. |
| Último inicio del sistema | La fecha y hora en que el dispositivo cliente se encendió por última vez. |
| Se debe reiniciar el dispositivo | Indicación de si se necesita reiniciar el dispositivo cliente. |
| Punto de distribución | El nombre del dispositivo que actúa como punto de distribución del dispositivo cliente. |
| Descripción | La descripción del dispositivo cliente recibida como resultado de un análisis de red. |
| Estado de cifrado | El estado del cifrado de datos en el dispositivo cliente. |
| Estado de WUA | El estado del Agente de Windows Update en el dispositivo cliente.<br>El valor *Sí* indica que el dispositivo cliente reciba las actualizaciones de Windows Update del Servidor de administración.<br>El valor *No* indica que el dispositivo cliente reciba las actualizaciones de Windows Update de otros orígenes. |
| Arquitectura del sistema operativo | La arquitectura del sistema operativo instalado en el dispositivo cliente. |
| Estado de protección antispam | El estado del componente de protección contra el spam: *En ejecución*, *Iniciándose*, *Detenida*, *En pausa*, *Error*, *Desconocido* |
| Estado de Prevención de fugas de datos | El estado del componente de prevención de fugas de datos: *En ejecución*, *Iniciándose*, *Detenida*, *En pausa*, *Error*, *Desconocido* |
| Estado de protección de los servidores de colaboración | El estado del componente de filtrado de contenido: *En ejecución*, *Iniciándose*, *Detenida*, *En pausa*, *Error*, *Desconocido* |
| Estado de protección antivirus en servidores de correo | El estado del componente de protección antivirus para servidores de correo: *En ejecución*, *Iniciándose*, *Detenida*, *En pausa*, *Error*, *Desconocido* |
| Estado de Sensor de Endpoint | El estado del componente Endpoint Detection and Response (KATA): *En ejecución*, *Iniciándose*, *Detenida*, *En pausa*, *Error*, *Desconocido* |
| Creado | El momento en el que se creó el icono <nombre del dispositivo>. Este atributo se utiliza para comparar varios eventos entre sí. |
| Nombre del Servidor de administración virtual o secundario | Nombre del Servidor de administración virtual o secundario. Esta columna solo está disponible en listas que contienen dispositivos de diferentes servidores de administración. |
| Grupo primario | El nombre del grupo de administración en el que se encuentra el icono <nombre del dispositivo>. Esta columna solo está disponible en listas que contienen dispositivos de diferentes servidores de administración. |

| Nombre de la columna | Valor |
|---|---|
| Administrado por un Servidor de administración diferente | Este parámetro puede tomar uno de estos valores:<br>• Verdadero, si, durante la instalación remota de aplicaciones de seguridad en el dispositivo, resulta que el dispositivo es administrado por un Servidor de administración diferente.<br>• Falso, en caso contrario. |
| Compilación del sistema operativo | Número de compilación del sistema operativo. Puede indicar si el número de compilación del sistema operativo seleccionado deberá ser igual, anterior o posterior al valor introducido. También puede hacer que la búsqueda incluya todos los números de compilación, excepto el especificado. |
| Id. de versión del sistema operativo | Identificador de versión del sistema operativo. Puede indicar si el sistema operativo seleccionado deberá tener un id. de versión igual, anterior o posterior al valor introducido. También puede hacer que la búsqueda incluya todos los id. de versión, excepto el especificado. |

# Estados de dispositivos, tareas y directivas

La tabla siguiente contiene una lista de iconos que aparecen en el árbol de consola y en el espacio de trabajo de la Consola de administración, junto a los nombres de los dispositivos, tareas y directivas. Estos iconos definen los estados de los objetos.

Estados de dispositivos, tareas y directivas

| Icono | Estado |
|---|---|
|  | Dispositivo con sistema operativo para estaciones de trabajo que se ha detectado en la red y no forma parte de ningún grupo de administración. |
|  | Dispositivo con sistema operativo para estaciones de trabajo que forma parte de un grupo de administración y tiene el estado *Sin inconvenientes*. |
|  | Dispositivo con sistema operativo para estaciones de trabajo que forma parte de un grupo de administración y tiene el estado *Advertencia*. |
|  | Dispositivo con sistema operativo para estaciones de trabajo que forma parte de un grupo de administración y tiene el estado *Crítico*. |
|  | Dispositivo con sistema operativo para estaciones de trabajo que forma parte de un grupo de administración y que ha perdido conexión con el Servidor de administración. |
|  | Dispositivo con sistema operativo para servidores que se ha detectado en la red y no forma parte de ningún grupo de administración. |
|  | Dispositivo con sistema operativo para servidores que forma parte de un grupo de administración y tiene el estado *Sin inconvenientes*. |
|  | Dispositivo con sistema operativo para servidores que forma parte de un grupo de administración y tiene el estado *Advertencia*. |
|  | Dispositivo con sistema operativo para servidores que forma parte de un grupo de administración y tiene el estado *Crítico*. |
|  | Dispositivo con sistema operativo para servidores que forma parte de un grupo de administración y que ha perdido conexión con el Servidor de administración. |
|  | Dispositivo móvil que se ha detectado en la red y que no forma parte de ningún grupo de administración. |
|  | Dispositivo móvil que forma parte de un grupo de administración y tiene el estado *Sin inconvenientes*. |
|  | Dispositivo móvil que forma parte de un grupo de administración y tiene el estado *Advertencia*. |
|  | Dispositivo móvil que forma parte de un grupo de administración y tiene el estado *Crítico*. |
|  | Dispositivo móvil que forma parte de un grupo de administración y que ha perdido conexión con el Servidor de administración. |
|  | Dispositivo con protección de UEFI que se ha detectado en la red y que no forma parte de ningún grupo de administración. El dispositivo con protección de UEFI se encuentra conectado a la red. |

| | |
|---|---|
|  | Dispositivo con protección de UEFI que se ha detectado en la red y que no forma parte de ningún grupo de administración. El dispositivo con protección de UEFI no está en la red. |
|  | Dispositivo con protección de UEFI que forma parte de un grupo de administración y tiene el estado *Sin inconvenientes*. El dispositivo con protección de UEFI está en la red. |
|  | Dispositivo con protección de UEFI que forma parte de un grupo de administración y tiene el estado *Sin inconvenientes*. El dispositivo con protección de UEFI no está en la red. |
|  | Dispositivo con protección de UEFI que forma parte de un grupo de administración y tiene el estado *Advertencia*. El dispositivo con protección de UEFI está en la red. |
|  | Dispositivo con protección de UEFI que forma parte de un grupo de administración y tiene el estado *Advertencia*. El dispositivo con protección de UEFI no está en la red. |
|  | Dispositivo con protección de UEFI que forma parte de un grupo de administración y tiene el estado *Crítico*. El dispositivo con protección de UEFI está en la red. |
|  | Dispositivo con protección de UEFI que forma parte de un grupo de administración y tiene el estado *Crítico*. El dispositivo con protección de UEFI no está en la red. |
|  | Directiva activa. |
|  | Directiva inactiva. |
|  | Directiva activa heredada de un grupo que se creó en el Servidor de administración principal. |
|  | Directiva activa heredada de un grupo de nivel superior. |
|  | Tarea (de grupo, del Servidor de administración o para dispositivos específicos) con el estado *Programada* o el estado *Completada correctamente*. |
|  | Tarea (de grupo, del Servidor de administración o para dispositivos específicos) con el estado *En ejecución*. |
|  | Tarea (de grupo, del Servidor de administración o para dispositivos específicos) con el estado *Error*. |
|  | Tarea heredada de un grupo que se creó en el Servidor de administración principal. |
|  | Tarea heredada de un grupo de nivel superior. |

# Icono de estado de archivo en la Consola de administración

Para facilitar la administración de archivos en la Consola de administración de Kaspersky Security Center, los iconos se muestran al lado de los nombres de archivos (consulte la siguiente tabla). Los iconos indican estados asignados a archivos por parte de aplicaciones de Kaspersky administradas en dispositivos cliente. Los iconos se muestran en los espacios de trabajo de las carpetas **Cuarentena**, **Copia de seguridad**, y **Amenazas activas**.

Los Estados son asignados a objetos por la Kaspersky Endpoint Security instalada en el dispositivo cliente en el cual el objeto se localiza.

Correspondencia entre iconos y estados de archivos

| Icono | Estado |
|---|---|
|  | Archivo con el estado *Infectado*. |
|  | Archivo con el estado *Advertencia* o *Probablemente infectado*. |
|  | Archivo con el estado *Agregado por el usuario*. |
|  | Archivo con el estado *Falso positivo*. |
|  | Archivo con el estado *Desinfectado*. |
|  | Archivo con el estado *Eliminado*. |

| | |
|---|---|
|  | Archivo en la carpeta **Cuarentena** con el estado *No infectado, Protegido con contraseña* o *Debe ser enviado a Kaspersky*. Si no hay descripción de estado al lado de un icono, esto significa que la Aplicación de Kaspersky administrada en el dispositivo cliente ha informado un estado desconocido a Kaspersky Security Center. |
|  | Archivo en la carpeta **Copia de seguridad** con el estado *No infectado, Protegido con contraseña* o *Debe ser enviado a Kaspersky*. Si no hay descripción de estado al lado de un icono, esto significa que la Aplicación de Kaspersky administrada en el dispositivo cliente ha informado un estado desconocido a Kaspersky Security Center. |
|  | Archivo en la carpeta **Amenazas activas** con el estado *No infectado, Protegido con contraseña* o *Debe ser enviado a Kaspersky*. Si no hay descripción de estado al lado de un icono, esto significa que la Aplicación de Kaspersky administrada en el dispositivo cliente ha informado un estado desconocido a Kaspersky Security Center. |

# Búsqueda y exportación de datos

Esta sección contiene la información sobre métodos de búsqueda de datos y sobre la exportación de datos.

## Búsqueda de dispositivos

Kaspersky Security Center le permite encontrar dispositivos según criterios especificados. Los resultados de la búsqueda serán guardados en un archivo de texto.

La función de búsqueda le permite encontrar los dispositivos siguientes:

- Dispositivos cliente en los grupos de administración del Servidor de administración y sus Servidores secundarios.
- Dispositivos no asignados administrados por un Servidor de administración y sus Servidores secundarios.

*Para encontrar dispositivos cliente incluidos en un grupo de administración:*

1. En el árbol de consola, seleccione una carpeta de grupo de administración.
2. Seleccione **Buscar** en el menú contextual de la carpeta del grupo de administración.
3. En las pestañas de la ventana **Buscar**, especifique los criterios para buscar dispositivos y luego haga clic en el botón **Buscar ahora**.

   Los dispositivos que cumplan con los criterios de búsqueda especificados ahora se muestran en una tabla en la parte inferior de la ventana **Buscar**.

*Para encontrar dispositivos no asignados:*

1. En el árbol de consola, seleccione la carpeta **Dispositivos no asignados**.
2. Seleccione **Buscar** en el menú contextual de la carpeta **Dispositivos no asignados**.
3. En las pestañas de la ventana **Buscar**, especifique los criterios para buscar dispositivos y luego haga clic en el botón **Buscar ahora**.

   Los dispositivos que cumplan con los criterios de búsqueda especificados ahora se muestran en una tabla en la parte inferior de la ventana **Buscar**.

*Para buscar dispositivos sin importar si están incluidos o no en un grupo de administración:*

1. En el árbol de consola, seleccione el nodo **Servidor de administración %s**.
2. En el menú contextual del nodo, seleccione **Buscar**.
3. En las pestañas de la ventana **Buscar**, especifique los criterios para buscar dispositivos y luego haga clic en el botón **Buscar ahora**.

   Los dispositivos que cumplan con los criterios de búsqueda especificados ahora se muestran en una tabla en la parte inferior de la ventana **Buscar**.

En la ventana **Buscar**, también puede buscar grupos de administración y Servidores de administración secundarios, usando una lista desplegable que se encuentra en la esquina superior derecha de la ventana. La búsqueda de funcionalidades de grupos de administración y Servidores de administración secundarios no está disponible si abrió la ventana **Buscar** desde la carpeta **Dispositivos no asignados**.

Para buscar dispositivos, puede usar expresiones regulares en los campos de la ventana **Buscar**.

La búsqueda de texto completo en la ventana **Buscar** está disponible:

- En la pestaña **Red**, en el campo **Descripción**.
- En la pestaña **Hardware**, en los campos **Dispositivo**, **Proveedor** y **Descripción**.

## Configuración de la búsqueda de dispositivos

A continuación, se describen los parámetros que se utilizan para buscar dispositivos administrados. Los resultados de búsqueda se muestran en la parte inferior de la ventana.

### Red

En la pestaña **Red**, puede especificar los criterios que se utilizarán para buscar dispositivos sobre la base de sus atributos de red:

- **Nombre o dirección IP del dispositivo**

  Nombre de red de Windows (nombre NetBIOS) del dispositivo, o la dirección IPv4 o IPv6.

- **Dominio de Windows**

  Muestra todos los dispositivos incluidos en el dominio de Windows especificado.

- **Grupo de administración**

  Muestra los dispositivos incluidos en el grupo de administración especificado.

- **Descripción**

  Texto ubicado en el campo **Descripción** de la sección **General** dentro de la ventana de propiedades del dispositivo.

  Para describir el texto del campo **Descripción**, puede utilizar los siguientes caracteres:

  - Dentro de una palabra:

    - *****. Sustituye una cadena de cualquier largo (es decir, con cualquier número de caracteres).

    **Ejemplo**:

    Para describir palabras como **Servidor** o **Servidores**, puede ingresar **Servidor***.

    - **?.** Sustituye un carácter individual.

    **Ejemplo**:

    Para describir palabras como **Window** o **Windows**, puede ingresar **Windo?**.

    La consulta no puede comenzar con un asterisco (*****) ni con un signo de interrogación (**?**).

  - Para encontrar varias palabras:

    - Espacio. Muestra todos los dispositivos que tienen, en su descripción, alguna de las palabras indicadas.

    **Ejemplo**:

    Para encontrar una frase que contenga las palabras **secundario** o **virtual**, puede incluir la expresión **secundario virtual** en la consulta.

    - **+**. Si agrega el signo + antes de una palabra, todos los resultados de búsqueda contendrán esa palabra.

    **Ejemplo**:

    Para encontrar una frase que contenga las palabras **secundario** y **virtual**, ingrese la consulta **+secundario+virtual**.

    - **-**. Si agrega el signo - antes de una palabra, ningún resultado de búsqueda contendrá esa palabra.

    **Ejemplo**:

    Para encontrar una frase que contenga **secundario** y no contenga **virtual**, ingrese la consulta **+secundario-virtual**.

    - **"<cadena>"**. El texto que se ingresa entre comillas debe estar presente en el texto.

    **Ejemplo**:

    Para encontrar una frase que contenga la combinación de palabras **servidor secundario**, puede ingresar **"servidor secundario"** en la consulta.

- Intervalo IP

  Si habilita esta opción, podrá ingresar las direcciones IP inicial y final del intervalo IP en el que deberán estar incluidos los dispositivos pertinentes.

  Esta opción está deshabilitada de forma predeterminada.

- Administrado por un Servidor de administración diferente

  Seleccione uno de los siguientes valores:

  - **Sí**. Solo se considerarán los dispositivos cliente administrados por otros Servidores de administración.
  - **No**. Solo se considerarán los dispositivos cliente administrados por el mismo Servidor de administración.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

## Etiquetas

En la pestaña **Etiquetas**, puede configurar una búsqueda de dispositivos que se base en palabras clave (etiquetas) agregadas de antemano a las descripciones de los dispositivos administrados:

- Aplicar si coincide al menos una etiqueta especificada

  Si habilita esta opción, los resultados de búsqueda mostrarán aquellos dispositivos que lleven, en su descripción, al menos una de las etiquetas seleccionadas.

  Si deshabilita esta opción, los resultados de búsqueda solo mostrarán aquellos dispositivos que no tengan ninguna de las etiquetas seleccionadas en su descripción.

  Esta opción está deshabilitada de forma predeterminada.

- La etiqueta debe incluirse

  Si selecciona esta opción, los resultados de búsqueda mostrarán aquellos dispositivos que lleven, en su descripción, la etiqueta seleccionada. La consulta de búsqueda puede incluir el asterisco, que representa una cadena de cualquier longitud (número de caracteres).

  Esta opción está seleccionada de manera predeterminada.

- La etiqueta debe excluirse

  Si selecciona esta opción, los resultados de búsqueda mostrarán aquellos dispositivos que no lleven en su descripción la etiqueta seleccionada. La consulta de búsqueda puede incluir el asterisco, que representa una cadena de cualquier longitud (número de caracteres).

## Active Directory

Utilice la pestaña **Active Directory** si desea que la búsqueda de dispositivos se lleve a cabo dentro de una unidad organizativa de Active Directory o de un grupo de Active Directory. La búsqueda puede abarcar las unidades organizativas secundarias de la unidad organizativa seleccionada. Para seleccionar los dispositivos, defina los siguientes ajustes:

- **El dispositivo está en una unidad organizativa de Active Directory**

  Si habilita esta opción, la selección incluirá los dispositivos de la unidad organizativa de Active Directory especificada en el campo de entrada.

  Esta opción está deshabilitada de forma predeterminada.

- **Incluir unidades de organización secundarias**

  Si habilita esta opción, la selección incluirá los dispositivos de todas las unidades organizativas secundarias de la unidad organizativa del dominio especificado.

  Esta opción está deshabilitada de forma predeterminada.

- **El dispositivo es miembro de un grupo de Active Directory**

  Si habilita esta opción, la selección incluirá los dispositivos que pertenezcan al grupo de Active Directory especificado en el campo de entrada.

  Esta opción está deshabilitada de forma predeterminada.

## Actividad de red

En la pestaña **Actividad de red**, puede especificar los criterios que se utilizarán para buscar dispositivos sobre la base de su actividad de red:

- El dispositivo es un punto de distribución

  En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

  - **Sí**. La selección incluirá dispositivos que funcionen como punto de distribución.
  - **No**. La selección no incluirá dispositivos que funcionen como punto de distribución.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

- No desconectar del Servidor de administración

  En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

  - **Habilitado**. La selección incluirá dispositivos en los que esté activada la casilla **No desconectar del Servidor de administración**.
  - **Deshabilitado**. La selección incluirá dispositivos en los que no esté activada la casilla **No desconectar del Servidor de administración**.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

- Perfil de conexión cambiado

  En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

  - **Sí**. La selección incluirá dispositivos que se hayan conectado al Servidor de administración tras un cambio de perfil de conexión.
  - **No**. La selección no incluirá dispositivos que se hayan conectado al Servidor de administración tras un cambio de perfil de conexión.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

- Última conexión con el Servidor de administración

  Puede utilizar esta casilla para establecer un criterio de búsqueda de dispositivos que se base en el momento en el que haya ocurrido la última conexión al Servidor de administración.

  Si activa esta casilla, podrá usar los campos de entrada para indicar el intervalo de tiempo (fecha y hora) en el que deberá haber ocurrido la última conexión entre el Agente de red instalado en el dispositivo cliente y el Servidor de administración. La selección incluirá aquellos dispositivos que estén alcanzados por el intervalo especificado.

  Si no activa esta casilla, no se aplicará este criterio.

  Esta casilla no está marcada de manera predeterminada.

- Nuevos dispositivos detectados por sondeo de red

  Utilice esta opción para buscar dispositivos nuevos, que se hayan detectado durante los sondeos de red realizados en días recientes.

  Si habilita esta opción, la selección incluirá solo aquellos dispositivos nuevos que se hayan detectado mediante el descubrimiento de dispositivos en el intervalo de días especificado en el campo **Periodo de detección (días)**.

  Si deshabilita esta opción, la selección incluirá todos los dispositivos detectados por el mecanismo de descubrimiento.

  Esta opción está deshabilitada de forma predeterminada.

- Dispositivo visible

  En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

  - **Sí**. La selección incluirá aquellos dispositivos que sean visibles en la red.
  - **No**. La selección incluirá aquellos dispositivos que no sean visibles en la red.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

## Aplicación

En la pestaña **Aplicación**, puede especificar los criterios que se usarán para buscar dispositivos basándose en los atributos de una aplicación administrada seleccionada:

- Nombre de la aplicación

  En la lista desplegable, puede definir un criterio para incluir dispositivos en la selección cuando se realice una basada en el nombre de una aplicación de Kaspersky.

  La lista solo contendrá los nombres de aquellas aplicaciones que tengan su respectivo complemento de administración instalado en la estación de trabajo del administrador.

  Si no selecciona ninguna aplicación, este criterio no se aplicará.

- Versión de la aplicación

  En el campo de entrada, puede definir un criterio para incluir dispositivos en la selección cuando se realice una búsqueda basada en el número de versión de una aplicación de Kaspersky.

  Si no especifica un número de versión, este criterio no se aplicará.

- Nombre de la actualización crítica

  En el campo de entrada, puede definir un criterio para incluir dispositivos en la selección cuando se realice una búsqueda basada en el nombre de una aplicación o en un número de paquete de actualización.

  Si el campo queda en blanco, este criterio no se aplicará.

- Última actualización de módulos

  Use esta opción para definir un criterio que permita buscar dispositivos según la hora en que se hayan actualizado por última vez los módulos de las aplicaciones instaladas en ellos.

  Si activa esta casilla, podrá utilizar los campos de entrada para definir el intervalo de tiempo (fecha y hora) en el que deberá haber ocurrido la última actualización de módulos de las aplicaciones instaladas en los dispositivos.

  Si no activa esta casilla, no se aplicará este criterio.

  Esta casilla no está marcada de manera predeterminada.

- El dispositivo se administra a través de Kaspersky Security Center

  Puede usar la lista desplegable para que la selección incluya aquellos dispositivos que se administren mediante Kaspersky Security Center:

  - **Sí**. La selección incluirá aquellos dispositivos que se administren mediante Kaspersky Security Center.
  - **No**. La aplicación incluirá aquellos dispositivos que no se administran mediante Kaspersky Security Center Linux.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

- La aplicación de seguridad está instalada

  Puede usar la lista desplegable para que la selección incluya aquellos dispositivos que tengan instalada la aplicación de seguridad:

  - **Sí**. La selección incluirá aquellos dispositivos en los que se haya instalado la aplicación de seguridad.
  - **No**. La selección incluirá aquellos dispositivos en los que no se haya instalado la aplicación de seguridad.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

## Sistema operativo

En la pestaña **Sistema operativo**, puede definir los siguientes criterios para buscar dispositivos basándose en el tipo de sistema operativo (SO):

- Versión del sistema operativo

  Si activa esta casilla, podrá seleccionar un sistema operativo de la lista. Los dispositivos que tengan instalado ese sistema operativo se incluirán en los resultados de búsqueda.

- Arquitectura del sistema operativo

  En la lista desplegable, puede seleccionar la arquitectura para la que deberá estar diseñado el sistema operativo. Los valores posibles son **Desconocido**, **x86**, **AMD64** e **IA64**. La arquitectura que elija determinará el modo de aplicar la regla de movimiento al dispositivo. De manera predeterminada, no hay ninguna opción seleccionada en la lista (es decir, la arquitectura del sistema operativo no está definida).

- **Versión de Service Pack del sistema operativo**

  En este campo, puede especificar la versión del paquete de su sistema operativo (en formato *X.Y*), que determinará cómo aplicar la regla de migración a su dispositivo. De manera predeterminada, no hay una versión definida.

- **Compilación del sistema operativo**

  Este parámetro solo es válido para sistemas operativos Windows.

  Número de compilación del sistema operativo. Puede indicar si el número de compilación del sistema operativo seleccionado deberá ser igual, anterior o posterior al valor introducido. También puede hacer que la búsqueda incluya todos los números de compilación, excepto el especificado.

- **Id. de versión del sistema operativo**

  Este parámetro solo es válido para sistemas operativos Windows.

  Identificador de versión del sistema operativo. Puede indicar si el sistema operativo seleccionado deberá tener un id. de versión igual, anterior o posterior al valor introducido. También puede hacer que la búsqueda incluya todos los id. de versión, excepto el especificado.

## Estado del dispositivo

En la pestaña **Estado del dispositivo**, puede definir criterios para buscar dispositivos basándose en el estado reportado para los mismos por una aplicación administrada:

- **Estado del dispositivo**

  Lista desplegable en la que puede seleccionar un estado de dispositivo: *Sin inconvenientes*, *Crítico* o *Advertencia*.

- **Estado de la protección en tiempo real**

  Lista desplegable en la cual puede seleccionar el estado de la protección en tiempo real. La selección incluirá aquellos dispositivos que tengan el estado de protección en tiempo real indicado.

- **Descripción del estado del dispositivo**

  En este campo, puede activar casillas correspondientes a condiciones que, al cumplirse, hacen que el dispositivo tome uno de los siguientes estados: *Sin inconvenientes*, *Crítico* o *Advertencia*.

- **Estado del dispositivo definido por la aplicación**

  Lista desplegable en la cual puede seleccionar el estado de la protección en tiempo real. La selección incluirá aquellos dispositivos que tengan el estado de protección en tiempo real indicado.

## Componentes de protección

En la pestaña **Componentes de protección**, puede configurar los criterios para buscar dispositivos cliente basándose en su estado de protección.

- **Bases de datos publicadas**

  Seleccione esta opción para buscar dispositivos cliente basándose en la fecha de publicación de las bases de datos antivirus. Utilice el campo de entrada para definir el intervalo de tiempo que se tomará como base para la búsqueda.

  Esta opción está deshabilitada de forma predeterminada.

- **Último análisis**

  Habilite esta opción para buscar dispositivos cliente basándose en la hora del último análisis antimalware. Utilice los campos de entrada para definir el período en el cual deberá haber ocurrido el último análisis antimalware.

  Esta opción está deshabilitada de forma predeterminada.

- **Número total de amenazas detectadas**

  Habilite esta opción para buscar dispositivos cliente basándose en el número de virus detectados. Utilice los campos de entrada para definir los valores que se tomarán como umbral superior e inferior del número de virus detectados.

  Esta opción está deshabilitada de forma predeterminada.

## Registro de aplicaciones

En la pestaña **Registro de aplicaciones**, puede configurar la búsqueda de dispositivos sobre la base de las aplicaciones que tienen instaladas:

- **Nombre de la aplicación**

  Lista desplegable en la que puede seleccionar una aplicación. Los dispositivos que tengan instalada la aplicación elegida se incluirán en la selección.

- **Versión de la aplicación**

  Campo de entrada en el que puede especificar la versión de la aplicación seleccionada.

- **Proveedor**

  Lista desplegable en la que puede seleccionar el desarrollador de una aplicación instalada en el dispositivo.

- **Estado de la aplicación**

  Lista desplegable en la que puede seleccionar el estado de la aplicación (*Instalada*, *Sin instalar*). Se incluirán en la selección los dispositivos que tengan o no tengan (dependiendo del estado seleccionado) la aplicación seleccionada.

- **Buscar por actualización**

  Si habilita esta opción, la búsqueda se basará en los detalles de las actualizaciones para el software instalado en los dispositivos pertinentes. Una vez que active esta casilla, los campos **Nombre de la aplicación**, **Versión de la aplicación** y **Estado de la aplicación** cambiarán a **Nombre de actualización**, **Versión de actualización** y **Estado**, respectivamente.

  Esta opción está deshabilitada de forma predeterminada.

- **Nombre de la aplicación de seguridad incompatible**

  Lista desplegable en la que puede seleccionar aplicaciones de seguridad de terceros. Los dispositivos que tengan instalada la aplicación seleccionada serán incluidos en la selección cuando se realice la búsqueda.

- **Etiqueta de aplicación**

  Lista desplegable en la que puede seleccionar una etiqueta de aplicación. Se incluirán en la selección aquellos dispositivos que tengan instaladas aplicaciones que, en su descripción, contengan la etiqueta seleccionada.

## Jerarquía de los Servidores de administración

En la pestaña **Jerarquía de los Servidores de administración**, active la casilla **Incluir datos de servidores de administración secundarios (hasta el nivel indicado)** si desea que, a la hora de buscar dispositivos, se tenga en cuenta la información almacenada en los servidores de administración secundarios. Utilice el campo de entrada para especificar el nivel de anidamiento máximo del que podrá provenir la información considerada. Esta casilla no está marcada de manera predeterminada.

## Máquinas virtuales

En la pestaña **Máquinas virtuales**, puede configurar la búsqueda de dispositivos basada en el hecho de que los dispositivos sean máquinas virtuales o formen parte de una VDI (infraestructura de escritorios virtuales):

- **Es una máquina virtual**

  En la lista desplegable puede seleccionar las siguientes opciones:

  - **No es importante**.
  - **No**. Buscar dispositivos que no sean máquinas virtuales.
  - **Sí**. Buscar dispositivos que sean máquinas virtuales.

- **Tipo de máquina virtual**

  En la lista desplegable, puede seleccionar el desarrollador de la máquina virtual.

  Esta lista desplegable estará disponible si seleccionó los valores **Sí** o **No es importante** en la lista desplegable **Es una máquina virtual**.

- **Parte de la infraestructura de escritorio virtual**

  En la lista desplegable puede seleccionar las siguientes opciones:

  - **No es importante**.
  - **No**. Buscar dispositivos que no sean parte de la Infraestructura de escritorio virtual.
  - **Sí**. Buscar dispositivos que sean parte de una VDI.

## Hardware

En la pestaña **Hardware**, puede configurar la búsqueda de dispositivos tomando como criterio sus características de hardware:

- **Dispositivo**

  En la lista desplegable, puede seleccionar un tipo de unidad. Los dispositivos que tengan la unidad seleccionada se incluirán en los resultados de búsqueda.

  El campo permite realizar búsquedas de texto completo.

- **Proveedor**

  En la lista desplegable, puede seleccionar el nombre del fabricante de la unidad. Los dispositivos que tengan la unidad seleccionada se incluirán en los resultados de búsqueda.

  El campo permite realizar búsquedas de texto completo.

- **Descripción**

  Descripción del dispositivo o unidad de hardware. Los dispositivos que tengan la descripción indicada en este campo se incluirán en la selección.

  Si desea agregar una descripción a un dispositivo, puede hacerlo (en cualquier formato) a través de la ventana de propiedades del mismo. El campo permite realizar búsquedas de texto completo.

- **Número de inventario**

  Los equipos que tengan el número de inventario indicado en este campo se incluirán en la selección.

- **Frecuencia de la CPU, en MHz**

  Intervalo de frecuencias de un procesador. La selección incluirá aquellos dispositivos que tengan un procesador con un intervalo de frecuencias comprendido en los límites dispuestos en los campos (inclusive).

- **Núcleos de CPU virtuales**

  Intervalo del número de núcleos virtuales de un procesador. La selección incluirá aquellos dispositivos que tengan un procesador comprendido en los límites dispuestos en los campos (inclusive).

- Volumen de disco duro, en GB

  Intervalo de valores referentes al tamaño del disco duro instalado en el dispositivo. La selección incluirá aquellos dispositivos que tengan un disco duro comprendido en los límites dispuestos en los campos (inclusive).

- Tamaño de RAM, en MB

  Rango de valores para el tamaño de la memoria RAM del dispositivo. Los dispositivos cuya memoria RAM coincida con los intervalos de estos campos de entrada (inclusive) se incluirán en la selección.

## Vulnerabilidades y actualizaciones

En la pestaña **Vulnerabilidades y actualizaciones**, puede configurar el criterio para buscar dispositivos según el origen de Windows Update que utilicen:

- WUA está ahora conectado al Servidor de administración

  En la lista desplegable, puede seleccionar una de las siguientes opciones de búsqueda:
  - **Sí**. Si selecciona esta opción, los resultados de búsqueda incluirán aquellos dispositivos que reciban sus actualizaciones de Windows Update del Servidor de administración.
  - **No**. Si selecciona esta opción, los resultados incluirán aquellos dispositivos que reciban sus actualizaciones de Windows Update de cualquier otro origen.

## Usuarios

En la pestaña **Usuarios**, puede configurar los criterios para buscar dispositivos basándose en las cuentas de usuario con las que se haya iniciado sesión en el sistema operativo.

- Último usuario que inició sesión en el sistema

  Si habilita esta opción, podrá hacer clic en el botón **Examinar** para seleccionar una cuenta de usuario. Los resultados de búsqueda incluirán aquellos dispositivos en los que el usuario indicado haya sido el último en iniciar sesión.

- Usuario que inició sesión en el sistema al menos una vez

  Si habilita esta opción, podrá hacer clic en el botón **Examinar** para seleccionar una cuenta de usuario. Los resultados de búsqueda incluirán aquellos dispositivos en los que el usuario indicado haya iniciado sesión al menos una vez.

## Problemas que afectan al estado en las aplicaciones administradas

En la pestaña **Problemas que afectan al estado en las aplicaciones administradas**, puede configurar la búsqueda de dispositivos según las descripciones de estado que brinda la aplicación administrada:

- **Descripción del estado del dispositivo**

  Puede activar casillas correspondientes a las descripciones de estado reportadas por la aplicación administrada. Cuando se reciban esos estados, los dispositivos correspondientes se incluirán en la selección. Si elige un estado incluido en las listas de varias aplicaciones, tendrá la opción de seleccionar todos los casos automáticamente.

## Estados de componentes en aplicaciones administradas

En la pestaña **Estados de componentes en aplicaciones administradas**, puede configurar criterios para buscar dispositivos según los estados de los componentes de las aplicaciones administradas:

- **Estado de Prevención de fugas de datos**

  Buscar dispositivos basándose en el estado de Prevención de fuga de datos (*Desconocido, Detenida, Iniciándose, En pausa, En ejecución, Error*).

- **Estado de protección de los servidores de colaboración**

  Buscar dispositivos basándose en el estado de la protección para servidores de colaboración (*Desconocido*, *Detenida*, *Iniciándose, En pausa*, *En ejecución*, *Error*).

- **Estado de protección antivirus en servidores de correo**

  Buscar dispositivos basándose en el estado de la protección para servidores de correo (*Desconocido, Detenida, Iniciándose, En pausa, En ejecución, Error).*

- **Estado de Sensor de Endpoint**

  Buscar dispositivos basándose en el estado del componente Sensor de Endpoint (*Desconocido, Detenida, Iniciándose, En pausa, En ejecución, Error*).

## Cifrado

- **Cifrado**

  Algoritmo de cifrado de bloque simétrico AES. En la lista desplegable, puede seleccionar el tamaño de la clave de cifrado (56 bits, 128 bits, 192 bits o 256 bits).

  Valores disponibles: *AES56*, *AES128*, *AES192* y *AES256*.

## Segmentos de nube

En la pestaña **Segmentos de nube**, puede configurar una búsqueda basada en los segmentos de nube a los que pertenece el dispositivo:

- **El dispositivo se encuentra en un segmento de nube**

  Si habilita esta opción, podrá hacer clic en el botón **Examinar** para seleccionar el segmento de búsqueda.

  Si también habilita la opción **Incluir objetos secundarios**, la búsqueda se realizará en todos los objetos secundarios del segmento elegido.

  Los resultados de la búsqueda solo incluirán aquellos dispositivos que estén en el segmento seleccionado.

- **Dispositivo encontrado mediante API**

  La lista desplegable le permite operar con el hecho de que el dispositivo pueda detectarse con las herramientas provistas por una API.

  - **AWS**. El dispositivo se descubre mediante la API de AWS, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de AWS.
  - **Azure**. El dispositivo se descubre mediante la API de Azure, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de Azure.
  - **Google Cloud.** El dispositivo se descubre utilizando la API de Google, es decir, el dispositivo está en el entorno de Google Cloud.
  - **No**. El dispositivo no se puede detectar con la API de AWS, Azure o Google (o bien el dispositivo no se encuentra en el entorno de nube, o bien sí está en el entorno de nube, pero, por algún motivo, no se lo puede detectar con una API).
  - **Ningún valor.** Esta condición no se aplica.

## Componentes de las aplicaciones

En esta sección, se enumeran los componentes de aquellas aplicaciones que tienen instalado un complemento de administración en la Consola de administración.

En la sección **Componentes de las aplicaciones**, puede definir criterios para incluir dispositivos en la selección basándose en los estados y los números de versión de los componentes vinculados a una aplicación seleccionada:

- **Estado**

  Buscar dispositivos basándose en el estado de un componente reportado por una aplicación al Servidor de administración. Puede seleccionar uno de los siguientes estados: *No hay datos del dispositivo*, *Detenido*, *Iniciándose*, *En pausa*, *En ejecución*, *Error de funcionamiento* y *Sin instalar*. Si el componente seleccionado de la aplicación instalada en un dispositivo administrado tiene el estado especificado, el dispositivo será incluido en la selección de dispositivos.

  Estados reportados por las aplicaciones:

  - *Iniciándose*: el componente está en proceso de iniciarse.
  - *En ejecución*: el componente está habilitado y funciona correctamente.
  - *En pausa*: el componente se encuentra suspendido (por ejemplo, porque el usuario pausó la protección en la aplicación administrada).
  - *Error de funcionamiento*: ocurrió un error durante el funcionamiento del componente.
  - *Detenido*: el componente está deshabilitado y no se encuentra en funcionamiento.
  - *Sin instalar*: el usuario no optó por instalar el componente al realizar una instalación personalizada de la aplicación.

  A diferencia de los demás estados, *No hay datos del dispositivo* no es un estado reportado por las aplicaciones. Se trata de una opción que muestra que las aplicaciones no tienen información sobre el estado del componente seleccionado. Esta situación puede presentarse, por ejemplo, cuando el componente seleccionado no pertenece a ninguna de las aplicaciones instaladas en el dispositivo o cuando el dispositivo está apagado.

- **Versión**

  Buscar dispositivos basándose en el número de versión del componente seleccionado en la lista. Puede escribir un número de versión, por ejemplo `3.4.1.0`, y luego especificar si el componente seleccionado debe tener una versión igual, anterior o posterior. También puede configurar la búsqueda de todas las versiones excepto la especificada.

## Uso de máscaras en variables de cadena

Se permite utilizar máscaras para las variables de cadena. Cuando se crean máscaras, puede utilizar las siguientes expresiones regulares:

- Carácter comodín (*): cualquier cadena de 0 o más caracteres.
- Signo de interrogación de cierre (?): cualquier carácter individual.
- [<rango>]: Reemplaza cualquier carácter individual dentro del rango o conjunto especificado.

  Por ejemplo, [0–9]: cualquier dígito; [abcdef]: cualquiera de los caracteres a, b, c, d, e, f.

# Uso de expresiones regulares en el campo de búsqueda

Puede usar las siguientes expresiones regulares en el campo de búsqueda para encontrar palabras y caracteres específicos:

- *. Reemplaza cualquier secuencia de caracteres. Para buscar palabras como Servidor, Servidores y Servidor de administración, escriba la expresión `Server*` en el campo de búsqueda.

- ?. Sustituye un carácter individual. Para buscar palabras como Casa o Capa, escriba la expresión `Ca?a` en el campo de búsqueda.

  > El texto en el campo de búsqueda no puede empezar con el signo de interrogación (?).

- [<rango>]. Reemplaza cualquier carácter individual dentro del rango o conjunto especificado. Para buscar cualquier dígito, ingrese la expresión `[0-9]` en el campo de búsqueda. Para buscar uno de los caracteres (a, b, c, d, e o f), ingrese la expresión `[abcdef]` en el campo de búsqueda.

Use las siguientes expresiones comunes en el campo de búsqueda para realizar una búsqueda de texto completo:

- Espacio. El resultado son todos los dispositivos cuyas descripciones contengan alguna de las palabras enumeradas. Por ejemplo, para buscar una frase que contenga la palabra "Secundario" o "Virtual" (o ambas), ingrese la expresión `Secundario Virtual` en el campo de búsqueda.

- Signo más (+), AND o &&. Si agrega el signo + antes de una palabra, todos los resultados de búsqueda contendrán esa palabra. Por ejemplo, para buscar una frase que contiene tanto la palabra "Secundario" como la palabra "Virtual", puede escribir cualquiera de las expresiones siguientes en el campo de búsqueda: `+Secundario+Virtual`, `Secundario AND Virtual`, `Secundario && Virtual`.

- OR o ||. Cuando se colocan entre dos palabras, indican que se puede encontrar una palabra o la otra en el texto. Para buscar una frase que contenga las palabras "Secundario" o "Virtual", escriba cualquiera de las siguientes expresiones en el campo de búsqueda: `Secundario OR Virtual`, `Secundario || Virtual`.

- Signo menos (-). Si agrega el signo - antes de una palabra, ningún resultado de búsqueda contendrá esa palabra. Para buscar una frase que deba contener la palabra Secundario y no deba contener la palabra Virtual, escriba la expresión `+Secundario-Virtual` en el campo de búsqueda.

- `"< algún texto >"`. El texto que se ingresa entre comillas debe estar presente en el texto. Para buscar una frase que contenga una combinación de palabras como "Servidor secundario", escriba la expresión `" Servidor secundario "` en el campo de búsqueda.

La búsqueda de texto completo está disponible en los siguientes bloques de filtrado:

- En el bloque de filtrado de la lista de eventos, en las columnas **Evento** y **Descripción**.

- En el bloque de filtrado de cuentas de usuarios, en la columna **Nombre**.

- En el bloque de filtrado de registros de aplicaciones, por la columna **Nombre**, si la sección **Mostrar en lista** tiene **no agrupar** seleccionada como criterio de filtración.

## Exportación de listas desde cuadros de diálogo

En los cuadros de diálogo de la aplicación, puede exportar listas de objetos a archivos de texto.

Es posible la exportación de una lista de objetos para las secciones de cuadros de diálogo que contienen el botón **Exportar a archivo**.

# Configuración de tareas

Esta sección enumera todas las configuraciones de tareas en Kaspersky Security Center.

## Configuración general de tareas

En esta sección, se enumeran los ajustes que puede ver y configurar en la mayoría de las tareas. La lista de ajustes disponibles depende de la tarea que se está configurando.

## Ajustes que se configuran al crear una tarea

A continuación, se enumeran los ajustes que puede definir al momento de crear una tarea. Algunos de estos ajustes también se pueden modificar en las propiedades de la tarea creada.

- Ajustes de reinicio del sistema operativo:
  - **No reiniciar el dispositivo**

    Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

  - **Reiniciar el dispositivo**

    Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

  - **Solicitar al usuario una acción**

    A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

    Esta opción está seleccionada de forma predeterminada.

  - **Repetir solicitud cada (min)**

    Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

    Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

    Si no habilita esta opción, la solicitud se mostrará una sola vez.

  - **Reiniciar después de (min)**

    Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

    Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

  - **Forzar el cierre de aplicaciones en sesiones bloqueadas**

Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

Esta opción está deshabilitada de forma predeterminada.

- Programación de la tarea:

  Los tipos de programación pueden variar según la tarea.

  - **Inicio programado (ajuste):**

    - Cada N horas

      La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

      De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

    - Cada N días

      La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

      De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

    - Cada N minutos

      La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

      De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

    - Por días de la semana

      La tarea se ejecutará periódicamente en los días de la semana y a la hora que indique.

      De manera predeterminada, la tarea se ejecutará todos los viernes a las 18:00:00.

    - Mensual

La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

- **Manual**

  La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

  Esta opción está seleccionada de forma predeterminada.

- **Una vez**

  La tarea se ejecuta una vez, en la fecha y hora especificadas (de manera predeterminada, el día en que se creó la tarea).

- **Inmediatamente**

  La tarea se ejecuta inmediatamente después de guardar su configuración.

- **Cada mes en los días especificados de semanas seleccionadas**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  Por defecto, la hora de inicio es a las 18:00 y no se selecciona ningún día del mes.

  Tenga en cuenta que no selecciona una fecha específica en el mes, ni el número de la semana (primera, segunda semana del mes), sino el número de secuencia del día de la semana dentro de un mes. Por ejemplo, si coloca el cursor en la celda **Ma** de la **Primero** fila, significa que la tarea se ejecutará el primer martes de cada mes nuevo.

  Puede seleccionar varios días de la semana.

- **Al descargar nuevas actualizaciones al repositorio**

  La tarea se ejecuta después de descargar las actualizaciones en el repositorio. Por ejemplo, es posible que desee utilizar este programa para la tarea de encontrar vulnerabilidades y actualizaciones necesarias.

- **Ante brotes de virus**

La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

- Antivirus para estaciones de trabajo y servidores de archivos
- Antivirus para defensa del perímetro
- Antivirus para sistemas de correo

Por defecto, están seleccionados todos los tipos de aplicaciones.

En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- Al completarse otra tarea

  La tarea actual se iniciará después de que se complete otra tarea. Esta opción solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

- Ejecutar tareas no realizadas

  Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

  Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

  Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

  Esta opción está deshabilitada de forma predeterminada.

- Esperar un tiempo definido al azar antes de iniciar la tarea

Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

- **Limitar el tiempo de espera a esta cantidad de minutos**

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

  Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

- Dispositivos a los que se asignará la tarea:
  - **Seleccionar dispositivos de la red detectados por el Servidor de administración**

    La tarea se asignará a ciertos dispositivos específicos. Estos pueden ser tanto dispositivos asignados a grupos de administración como dispositivos no asignados.

    Podría usar esta opción para, por ejemplo, una tarea que instale el Agente de red en los dispositivos que no estén asignados a un grupo de administración.

  - **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**

    Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

    Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.

  - **Asignar tarea a una selección de dispositivos**

    La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

    Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

  - **Asignar tarea a un grupo de administración**

    La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

    Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

    Si se asigna una tarea a un grupo de administración, la pestaña **Seguridad** no se muestra en la ventana de propiedades de la tarea porque las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

- Ajustes de cuenta:
  - **Cuenta predeterminada**

    La tarea se ejecutará utilizando la misma cuenta que la aplicación que realizará la tarea.

    Esta opción está seleccionada de forma predeterminada.

  - **Especificar cuenta**

    Complete los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta con la que se ejecutará la tarea. La cuenta debe tener los derechos necesarios para realizar la tarea.

  - **Cuenta**

Cuenta con la que se ejecutará la tarea.

- **Contraseña**

  Contraseña de la cuenta con la que se ejecutará la tarea.

Si el Agente de red no está instalado en el dispositivo de destino, debe especificar la cuenta que se utilizará en el dispositivo de destino para acceder al recurso compartido admin $. La cuenta que especifique solo está destinada a copiar los datos a su dispositivo. Si el Agente de red está instalado en el dispositivo de destino, los datos se copian a través del Agente de red y no tiene que especificar ninguna cuenta al crear la tarea.

## Ajustes que se configuran tras crear una tarea

Los siguientes ajustes pueden definirse solamente cuando la tarea ya se ha creado.

- Ajustes para tareas de grupo:
  - **Distribuir a subgrupos**

    Esta opción solo está disponible en los ajustes de tareas de grupo.

    Cuando esta opción está habilitada, el alcance de la tarea incluye lo siguiente:

    - El grupo de administración que se seleccionó al crear la tarea.
    - Los grupos de administración subordinados al grupo de administración seleccionado y ubicados en cualquier nivel de la jerarquía de grupos.

    Cuando esta opción está deshabilitada, el alcance de la tarea incluye solo el grupo de administración que se seleccionó al crear la tarea.

    Esta opción está activada de forma predeterminada.

  - **Distribuir a servidores de administración secundarios y virtuales**

    Cuando esta opción está habilitada, la tarea aplicada al Servidor de administración principal se aplica también a los servidores de administración secundarios (incluidos los virtuales). Si ya existe una tarea del mismo tipo en un Servidor de administración secundario, se aplican ambas tareas a ese servidor (la existente y la heredada del Servidor de administración principal).

    Esta opción solo está disponible cuando la opción **Distribuir a subgrupos** está habilitada.

    Esta opción está deshabilitada de forma predeterminada.

- Ajustes de programación avanzados:
  - **Encender dispositivos mediante la función Wake-on-LAN antes de iniciar la tarea (min)**

    El sistema operativo del dispositivo se iniciará a la hora especificada antes de que se ejecute la tarea. El período de tiempo predeterminado es de cinco minutos.

    Habilite esta opción si desea que la tarea se ejecute en todos los dispositivos cliente que formen parte del alcance de la tarea, incluidos aquellos que se encuentren apagados cuando la tarea esté próxima a comenzar.

    Si desea que el dispositivo se apague automáticamente una vez completada la tarea, habilite la opción **Apagar dispositivos cuando se complete la tarea**. Encontrará esta opción en la misma ventana.

    Esta opción está deshabilitada de forma predeterminada.

  - **Apagar dispositivos cuando se complete la tarea**

    Esta opción puede ser útil para, por ejemplo, una tarea que actualice los dispositivos cliente todos los viernes después del horario laboral y luego los apague para que no consuman energía el fin de semana.

    Esta opción está deshabilitada de forma predeterminada.

- Detener la tarea si tarda más de (min)

  Una vez que transcurra el período especificado, la tarea se detendrá automáticamente, se haya completado o no.

  Habilite esta opción si desea que las tareas que tarden mucho en completarse se interrumpan o se detengan.

  Esta opción está deshabilitada de forma predeterminada. El tiempo de ejecución por defecto para las tareas es de 120 minutos.

- Ajustes de notificaciones:
  - Bloque **Almacenar el historial de la tarea**:
    - Guardar en el Servidor de administración por (días)

      El Servidor de administración conservará por el número de días especificado los eventos de la aplicación que estén relacionados con la ejecución de la tarea en los dispositivos cliente incluidos en el alcance de la tarea. Transcurrido este período, la información se eliminará del Servidor de administración.

      Esta opción está activada de forma predeterminada.

    - Guardar en el registro de eventos del SO del dispositivo

      Los eventos de la aplicación relacionados con la ejecución de la tarea se almacenarán localmente en el registro de eventos de Windows de cada dispositivo cliente.

      Esta opción está deshabilitada de forma predeterminada.

    - Guardar en el registro de eventos del Servidor de administración

      Los eventos de la aplicación que estén relacionados con la ejecución de la tarea en los dispositivos cliente incluidos en el alcance de la tarea se almacenarán centralmente, en el registro de eventos de Windows del equipo en el que esté instalado el Servidor de administración.

      Esta opción está deshabilitada de forma predeterminada.

    - Guardar todos los eventos

      Si selecciona esta opción, se guardarán todos los sucesos vinculados a la tarea en los registros de eventos.

    - Guardar eventos sobre el progreso de la tarea

      Si selecciona esta opción, se guardarán solo aquellos sucesos que estén vinculados con la ejecución de la tarea en los registros de eventos.

    - Guardar solo los resultados de la ejecución de la tarea

      Si selecciona esta opción, se guardarán solo aquellos sucesos que estén vinculados con los resultados de la tarea en los registros de eventos.

  - Notificar los resultados de ejecución de la tarea al administrador

    Puede seleccionar los métodos que se usarán para notificar a los administradores sobre los resultados de la ejecución de la tarea. Los métodos posibles son el correo electrónico, los mensajes SMS y la ejecución de un archivo. Para configurar el mecanismo de notificación, haga clic en el vínculo **Configuración**.

    De forma predeterminada, todos los métodos de notificación están deshabilitados.

- Notificar solo acerca de los errores

  Si esta opción está habilitada, los administradores recibirán una notificación solo si ocurre un error al ejecutar la tarea.

  Si esta opción está deshabilitada, los administradores recibirán una notificación cada vez que se complete la tarea.

  Esta opción está activada de forma predeterminada.

- Ajustes de seguridad
- Ajustes del alcance de la tarea

  Dependiendo de cómo se determine el alcance de la tarea, estarán presentes los siguientes ajustes:

  - Dispositivos

    Si el alcance de la tarea está determinado por un grupo de administración, verá el nombre del grupo. No podrá hacer ningún cambio. Sin embargo, podrá configurar **Exclusiones del alcance de la tarea**.

    Si el alcance de la tarea está determinado por una lista de dispositivos, podrá agregar y eliminar dispositivos en la lista.

  - Selección de dispositivos

    Podrá cambiar la selección de dispositivos a la que se aplicará la tarea.

  - Exclusiones del alcance de la tarea

    Podrá definir grupos de dispositivos a los que no se aplicará la tarea. Los grupos excluidos solo pueden ser subgrupos del grupo de administración al que se aplica la tarea.

- **Historial de revisiones**

# Ajustes de la tarea Descargar actualizaciones en el repositorio del Servidor de administración

## Ajustes que se configuran al crear una tarea

A continuación, se enumeran los ajustes que puede definir al momento de crear una tarea. Algunos de estos ajustes también se pueden modificar en las propiedades de la tarea creada.

- Orígenes de actualizaciones

  Los siguientes recursos pueden utilizarse como orígenes de actualizaciones para el Servidor de administración:

  - Servidores de actualizaciones de Kaspersky

    Servidores HTTP(S) de Kaspersky desde los que las aplicaciones de Kaspersky descargan actualizaciones para sus bases de datos y módulos de software. De forma predeterminada, el Servidor de administración utiliza el protocolo HTTPS para comunicarse con los servidores de actualizaciones de Kaspersky y descargar las actualizaciones. Si lo desea, puede hacer que el Servidor de administración utilice el protocolo HTTP en lugar del protocolo HTTPS.

    Esta es la opción seleccionada por defecto.

  - Servidor de administración principal

    Este recurso se aplica a las tareas creadas para un Servidor de administración secundario o virtual.

  - Carpeta local o de red

    Una carpeta local o de red con las últimas actualizaciones. La carpeta de red puede ser un servidor FTP o HTTP, o un recurso compartido SMB. Si el acceso a la carpeta requiere autenticación, solo puede usarse el protocolo SMB. La carpeta local debe ser una carpeta del dispositivo en el que se encuentra instalado el Servidor de administración.

    El servidor FTP/HTTP o la carpeta de red utilizada por un origen de actualizaciones debe contener una estructura de carpetas (con actualizaciones) que coincida con la estructura que se crea al usar los servidores de actualizaciones de Kaspersky.

- **Otras opciones**

  Forzar actualización de los servidores de administración secundarios

  Si esta opción está habilitada, el Servidor de administración iniciará las tareas de actualización en los servidores de administración secundarios en cuanto se descarguen nuevas actualizaciones. Las tareas de actualización se inician utilizando el origen de actualización configurado en las propiedades de la tarea en los Servidores de administración secundarios.

  Si esta opción no está habilitada, las tareas de actualización se iniciarán en los Servidores de administración secundarios siguiendo lo que indiquen sus programaciones.

  Esta opción está deshabilitada de forma predeterminada.

  Copiar actualizaciones descargadas a carpetas adicionales

Una vez que el Servidor de administración recibe actualizaciones, las copiará a las carpetas especificadas. Utilice esta opción si desea controlar manualmente la distribución de actualizaciones en la red.

Podría utilizar esta opción en, por ejemplo, la siguiente situación: la red de su organización está formada por varias subredes independientes. Los dispositivos de cada subred no tienen acceso a las demás subredes. Sin embargo, los dispositivos de todas las subredes tienen acceso a una misma carpeta compartida. En un caso así, puede hacer que el Servidor de administración de una subred descargue las actualizaciones de los servidores de actualizaciones de Kaspersky, habilitar esta opción y definir esa carpeta compartida como destino. Luego, defina esa carpeta como origen de actualizaciones en las tareas "Descargar actualizaciones en el repositorio del Servidor de administración" de los demás servidores de administración.

Si selecciona copiar las actualizaciones descargadas a una carpeta local, debe especificar una carpeta en el dispositivo que tiene el Servidor de administración instalado. La ruta a la carpeta depende del sistema operativo del dispositivo. Dado que la carpeta local se encuentra en el Servidor de administración basado en Linux, debe especificar la ruta POSIX, por ejemplo: /path/to/dir.

Cuando selecciona una carpeta de red que se encuentra en el Servidor de administración basado en Linux, debe montar la carpeta para garantizar el acceso a la carpeta de red con anticipación desde el dispositivo que tiene el Servidor de administración. El acceso a la carpeta se realiza mediante el protocolo de SMB.

Esta opción está deshabilitada de forma predeterminada.

**No forzar la actualización de los dispositivos y de los servidores de administración secundarios si la copia no se ha completado**

Las tareas para descargas actualizaciones en los dispositivos cliente y en los servidores de administración secundarios no se iniciarán hasta que las actualizaciones hayan terminado de copiarse de la carpeta de actualización principal a las carpetas de actualización adicionales.

Debe habilitar esta opción si sus dispositivos cliente y sus servidores de administración secundarios obtienen sus actualizaciones de carpetas de red adicionales.

Esta opción está deshabilitada de forma predeterminada.

## Ajustes que se configuran tras crear una tarea

Los siguientes ajustes pueden definirse solamente cuando la tarea ya se ha creado.

- Bloquee la sección **Configuración**, **Contenido de las actualizaciones**

  **Descargar archivos diff**

  Esta opción habilita la función de descarga de archivos diff.

  Esta opción está deshabilitada de forma predeterminada.

- Sección **Verificación de actualizaciones**

  **Verificar actualizaciones antes de distribuirlas**

  El Servidor de administración descarga las actualizaciones del origen, las guarda en un repositorio temporal y ejecuta la tarea definida en el campo **Tarea de verificación de actualizaciones**. Si la tarea se completa con éxito, las actualizaciones se copian desde el repositorio temporal a una carpeta compartida en el Servidor de administración y luego se distribuyen a todos los dispositivos para los cuales el Servidor de administración actúa como fuente de actualizaciones (tareas con el tipo de programación **Al descargar nuevas actualizaciones al repositorio** empezada). La tarea para descargar las actualizaciones en el repositorio terminará solo luego de que se complete la tarea *Verificación de actualizaciones*.

  Esta opción está deshabilitada de forma predeterminada.

  **Tarea de verificación de actualizaciones**

  Esta tarea verifica las actualizaciones descargadas antes de que se distribuyan a todos los dispositivos para los cuales el Servidor de administración actúa como fuente de actualizaciones.

  En este campo, puede seleccionar la tarea *Verificación de actualizaciones* creada anteriormente. Como alternativa, puede crear una tarea *Verificación de actualizaciones* nueva.

# Configuración de la tarea Descargar actualizaciones en los repositorios de los puntos de distribución

## Ajustes que se configuran al crear una tarea

A continuación, se enumeran los ajustes que puede definir al momento de crear una tarea. Algunos de estos ajustes también se pueden modificar en las propiedades de la tarea creada.

- **Orígenes de actualizaciones**

  Los siguientes recursos se pueden utilizar como orígenes de actualizaciones para el punto de distribución:

  - Servidores de actualizaciones de Kaspersky

    Servidores HTTP(S) de Kaspersky desde los que las aplicaciones de Kaspersky descargan actualizaciones para sus bases de datos y módulos de software.

    Esta opción está seleccionada de forma predeterminada.

  - Servidor de administración principal

    Este recurso se aplica a las tareas creadas para un Servidor de administración secundario o virtual.

  - Carpeta local o de red

    Una carpeta local o de red con las últimas actualizaciones. La carpeta de red puede ser un servidor FTP o HTTP, o un recurso compartido SMB. Si el acceso a la carpeta requiere autenticación, solo puede usarse el protocolo SMB. La carpeta local debe ser una carpeta del dispositivo en el que se encuentra instalado el Servidor de administración.

    El servidor FTP/HTTP o la carpeta de red utilizada por un origen de actualizaciones debe contener una estructura de carpetas (con actualizaciones) que coincida con la estructura que se crea al usar los servidores de actualizaciones de Kaspersky.

- **Otras opciones** → **Carpeta para almacenar actualizaciones**

  La ruta a la carpeta especificada para almacenar las actualizaciones guardadas. Puede copiar la ruta de la carpeta especificada en el portapapeles. No puede cambiar la ruta a una carpeta específica para una tarea de grupo.

## Ajustes que se configuran tras crear una tarea

Puede especificar la siguiente configuración en la sección **Configuración**, en el bloque **Contenido de las actualizaciones**, solo tras crear una tarea.

**Descargar archivos diff**

Esta opción habilita la función de descarga de archivos diff.

Esta opción está deshabilitada de forma predeterminada.

# Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

## Ajustes que se configuran al crear una tarea

A continuación, se enumeran los ajustes que puede definir al momento de crear una tarea. Algunos de estos ajustes también se pueden modificar en las propiedades de la tarea creada.

- **Buscar vulnerabilidades y actualizaciones catalogadas por Microsoft**

  Al buscar vulnerabilidades y actualizaciones, Kaspersky Security Center utiliza la información sobre las actualizaciones de Microsoft aplicables desde la fuente de actualizaciones de Microsoft, las cuales están disponibles en este momento.

  Podría deshabilitar esta opción si, por ejemplo, ha creado tareas diferentes (con configuraciones diferentes) para las actualizaciones de Microsoft y para las actualizaciones de aplicaciones de terceros.

  Esta opción está activada de forma predeterminada.

  La información sobre las actualizaciones opcionales de Microsoft Windows no se envía al Servidor de administración.

  - **Conectarse al servidor de actualizaciones para actualizar los datos**

El Agente de Windows Update del dispositivo administrado se conectará al origen de actualizaciones de Microsoft. Los siguientes servidores pueden actuar como orígenes de actualizaciones de Microsoft:

- Servidor de administración de Kaspersky Security Center (consulte la configuración de la directiva del Agente de red)
- Un servidor Windows Server con Microsoft Windows Server Update Services (WSUS) que se encuentre instalado en la red de su organización
- Los servidores de actualizaciones de Microsoft

Cuando esta opción está habilitada, el Agente de Windows Update del dispositivo administrado se conecta al origen de actualizaciones de Microsoft para obtener información actualizada sobre las actualizaciones de Microsoft Windows aplicables.

Cuando esta opción está deshabilitada, el Agente de actualización de Windows del dispositivo administrado usa la información sobre las actualizaciones de Microsoft Windows aplicables que el origen de actualizaciones brindó en un momento anterior.

Conectarse al origen de actualizaciones de Microsoft puede consumir muchos recursos. Podría deshabilitar esta opción si ha configurado un esquema de conexión periódica a este origen en otra tarea o en la sección **Actualizaciones y vulnerabilidades de software** de las propiedades de la directiva del Agente de red. Si no quiere deshabilitar esta opción, para intentar que el Servidor de administración no se sobrecargue, modifique la programación de la tarea para que se la inicie en un punto aleatorio de un intervalo de 360 minutos.

Esta opción está activada de forma predeterminada.

El modo de obtener las actualizaciones deriva de combinar las siguientes opciones de configuración de la directiva del Agente de red:

- El Agente de Windows Update en un dispositivo administrado se conecta al Servidor de actualizaciones para obtener actualizaciones solo si la opción **Conectarse al servidor de actualizaciones para actualizar los datos** está activada en las propiedades de la tarea *Buscar vulnerabilidades y actualizaciones requeridas* y la opción de **Modo de búsqueda de Windows Update** está configurada como **Activo** en la configuración de la directiva del Agente de red.
- Si no necesita el Agente de red para iniciar una conexión al origen de actualizaciones de Microsoft Windows ni para descargar actualizaciones al realizar la tarea *Análisis de vulnerabilidades*, puede seleccionar la opción **Pasivo** en **Modo de búsqueda de Windows Update**, pero la opción **Conectarse al servidor de actualizaciones para actualizar los datos** debe permanecer habilitada. Así podrá ahorrar recursos y usar las actualizaciones de Windows antes recibidas para analizar las vulnerabilidades. Puede usar el modo pasivo si configura la recepción de actualizaciones de Microsoft Windows de otra manera. Si la recepción de actualizaciones de Microsoft Windows no está configurada de otra manera, no seleccione la opción **Pasivo** en **Modo de búsqueda de Windows Update** porque, en este caso, nunca recibirá información sobre las actualizaciones.
- Independientemente del estado de la opción **Conectarse al servidor de actualizaciones para actualizar los datos** (habilitado o deshabilitado), si se selecciona la opción **Modo de búsqueda de Windows Update** en **Deshabilitado**, Kaspersky Security Center no solicita ninguna información sobre actualizaciones.

- Buscar vulnerabilidades y actualizaciones catalogadas por Kaspersky para software de terceros

Si esta opción está habilitada, Kaspersky Security Center busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft) en el Registro de Windows y en las carpetas especificadas en **Especifique las rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**. Kaspersky determina el alcance de la lista de aplicaciones de terceros compatibles.

Si esta opción está deshabilitada, Kaspersky Security Center no busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros. Puede que quiera deshabilitar esta opción si utiliza tareas diferentes, con configuraciones diferentes, para las actualizaciones de Microsoft Windows y para las actualizaciones de aplicaciones de terceros.

Esta opción está activada de forma predeterminada.

- **Especifique las rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**

  Carpetas en las que Kaspersky Security Center buscará aplicaciones de terceros que requieran la instalación de actualizaciones o que tengan vulnerabilidades que deban repararse. Puede utilizar variables del sistema.

  Especifique las carpetas en las que se instalan las aplicaciones. De forma predeterminada, la lista contiene carpetas del sistema en las que se instalan la mayoría de las aplicaciones.

- **Habilitar diagnóstico avanzado**

  Si esta función está habilitada, el Agente de red escribe archivos de seguimiento, incluso si la escritura de archivos de seguimiento está deshabilitada para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center. Los datos de seguimiento se guardan en dos archivos sucesivamente; el tamaño total de ambos archivos está determinado por el valor de la opción **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando los archivos alcanzan su límite de tamaño, el Agente de red comienza a sobrescribirlos. Los archivos de seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

  Si esta función está deshabilitada, el Agente de red escribe rastreos de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center. No se guardará ningún otro dato de seguimiento.

  No es necesario que habilite la característica de diagnóstico avanzado al momento de crear una tarea. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

  Esta opción está deshabilitada de forma predeterminada.

- **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Los especialistas en soporte técnico de Kaspersky podrían pedirle que cambie el valor predeterminado si, para solucionar un problema, les remite archivos de diagnóstico avanzado con información insuficiente.

# Configuración de la tarea Instalar actualizaciones requeridas y corregir vulnerabilidades

## Ajustes que se configuran al crear una tarea

A continuación, se enumeran los ajustes que puede definir al momento de crear una tarea. Algunos de estos ajustes también se pueden modificar en las propiedades de la tarea creada.

- **Elija las reglas de instalación de actualizaciones**

  Estas reglas se aplican a la instalación de actualizaciones en dispositivos cliente. Si no se especifican las reglas, la tarea no tiene nada que realizar. Para obtener información sobre las operaciones con reglas, consulte Reglas para la instalación de actualizaciones.

- **Comenzar instalación cuando se esté por reiniciar o apagar el dispositivo**

  Si esta opción está habilitada, las actualizaciones se instalarán en el momento en el que los dispositivos se reinicien o se apaguen. De lo contrario, las actualizaciones se instalarán siguiendo la programación que se defina.

  Utilice esta opción si la instalación de las actualizaciones podría afectar el rendimiento de los dispositivos.

  Esta opción está deshabilitada de forma predeterminada.

- **Instalar los componentes requeridos y generales del sistema**

  Si esta opción está habilitada, antes de que se instale una actualización, la aplicación instalará automáticamente todos los componentes generales del sistema que la actualización requiera para instalarse (los llamados "requisitos previos"). Una actualización podría requerir, por ejemplo, que esté instalada cierta actualización del sistema operativo.

  Si esta opción está deshabilitada, posiblemente tenga que instalar los requisitos previos manualmente.

  Esta opción está deshabilitada de forma predeterminada.

- **Permitir la instalación de versiones nuevas de aplicaciones durante las actualizaciones**

  Si esta opción está habilitada, las actualizaciones podrán cambiar la versión del software actualizado por una más reciente.

  Si esta opción está deshabilitada, los cambios de versión no estarán permitidos. Para instalar una versión más reciente de una aplicación, deberá usar una tarea diferente o proceder en forma manual. Podría usar esta opción si, por ejemplo, desea evaluar el cambio de versión en una infraestructura de prueba o si sabe que la versión más reciente no es compatible con la infraestructura de su empresa.

  Esta opción está activada de forma predeterminada.

  Los cambios de versión pueden ocasionar problemas de funcionamiento en las aplicaciones dependientes instaladas en los dispositivos cliente.

- **Descargar actualizaciones en el dispositivo sin instalarlas**

  Si esta opción está habilitada, la aplicación descargará las actualizaciones disponibles en los dispositivos, pero no las instalará automáticamente. Podrá instalar las actualizaciones descargadas manualmente.

  Las actualizaciones de Microsoft se descargan en el sistema de almacenamiento de Windows. Las actualizaciones para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky ni Microsoft) se descargan en la carpeta especificada en el campo **Descargar actualizaciones en**.

  Si esta opción está deshabilitada, las actualizaciones se instalarán en los dispositivos automáticamente.

  Esta opción está deshabilitada de forma predeterminada.

  - **Descargar actualizaciones en**

    Esta carpeta se utiliza para descargar las actualizaciones para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky ni Microsoft).

- **Habilitar diagnóstico avanzado**

  Si esta función está habilitada, el Agente de red escribe archivos de seguimiento, incluso si la escritura de archivos de seguimiento está deshabilitada para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center. Los datos de seguimiento se guardan en dos archivos sucesivamente; el tamaño total de ambos archivos está determinado por el valor de la opción **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando los archivos alcanzan su límite de tamaño, el Agente de red comienza a sobrescribirlos. Los archivos de seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

  Si esta función está deshabilitada, el Agente de red escribe rastreos de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center. No se guardará ningún otro dato de seguimiento.

  No es necesario que habilite la característica de diagnóstico avanzado al momento de crear una tarea. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

  Esta opción está deshabilitada de forma predeterminada.

  - **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

    El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Los especialistas en soporte técnico de Kaspersky podrían pedirle que cambie el valor predeterminado si, para solucionar un problema, les remite archivos de diagnóstico avanzado con información insuficiente.

## Ajustes que se configuran tras crear una tarea

Puede especificar los ajustes en las siguientes listas cuando la tarea ya se creó. Para obtener una descripción completa de la configuración de tareas, consulte Configuración general de la tareas.

- **General**. En esta sección se muestra información general sobre la tarea. Además, puede especificar a qué dispositivos se debe aplicar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*:

  - **Distribuir a subgrupos**

    Esta opción solo está disponible en los ajustes de tareas de grupo.

    Cuando esta opción está habilitada, el alcance de la tarea incluye lo siguiente:

    - El grupo de administración que se seleccionó al crear la tarea.
    - Los grupos de administración subordinados al grupo de administración seleccionado y ubicados en cualquier nivel de la jerarquía de grupos.

    Cuando esta opción está deshabilitada, el alcance de la tarea incluye solo el grupo de administración que se seleccionó al crear la tarea.

    Esta opción está activada de forma predeterminada.

  - **Distribuir a servidores de administración secundarios y virtuales**

    Cuando esta opción está habilitada, la tarea aplicada al Servidor de administración principal se aplica también a los servidores de administración secundarios (incluidos los virtuales). Si ya existe una tarea del mismo tipo en un Servidor de administración secundario, se aplican ambas tareas a ese servidor (la existente y la heredada del Servidor de administración principal).

    Esta opción solo está disponible cuando la opción **Distribuir a subgrupos** está habilitada.

    Esta opción está deshabilitada de forma predeterminada.

- Actualizaciones para instalar

  En la sección **Actualizaciones para instalar**, puede ver la lista de actualizaciones instaladas por la tarea. Solo se muestran las actualizaciones que coinciden con la configuración de la tarea aplicada.

- Prueba de instalación de actualizaciones:

  - **No analizar**. Seleccione esta opción si no desea realizar una instalación de prueba de las actualizaciones.
  - **Ejecutar análisis en los dispositivos seleccionados**. Seleccione esta opción si desea probar la instalación de actualizaciones en dispositivos seleccionados. Haga clic en el botón **Agregar** y seleccione los dispositivos en los que necesita realizar una instalación de prueba de las actualizaciones.
  - **Ejecutar análisis en los dispositivos del grupo especificado**. Seleccione esta opción si desea probar la instalación de actualizaciones en un grupo de dispositivos. En el campo **Especifique un grupo de prueba**, indique un grupo de dispositivos en el que desee realizar una instalación de prueba.
  - **Ejecutar análisis en el porcentaje de dispositivos especificado**. Seleccione esta opción si desea probar la instalación de actualizaciones en una parte de los dispositivos. En el campo **Porcentaje de dispositivos de prueba en relación con todos los dispositivos de destino**, especifique el porcentaje de dispositivos en el que desea realizar una instalación de prueba de las actualizaciones.

# Lista global de subredes

Esta sección proporciona información sobre la lista global de subredes que puede usar en las reglas.

Para almacenar la información sobre las subredes de su red, puede configurar una lista global de subredes para cada Servidor de administración que utilice. Esta lista le ayuda a hacer coincidir los pares {dirección IP, máscara} y unidades físicas y sucursales. Puede usar subredes de esta lista en las reglas y configuraciones de red.

## Añadir subredes a la lista global de subredes

Puede agregar subredes con sus descripciones a la lista global de subredes.

*Para añadir subredes a la lista global de subredes:*

1. En el árbol de la consola, seleccione el nodo del Servidor de administración con el que desee trabajar.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
3. En la ventana **Propiedades** que se abre, en el panel **Secciones**, seleccione **Lista de subredes globales**.
4. Haga clic en el botón **Agregar**.

   Se abre la ventana **Nueva subred**.
5. Complete los siguientes campos:

   - **Configuración general**

     La dirección IP de subred para la subred que está agregando.

   - **Máscara de subred**

     La máscara de subred para la subred que está añadiendo.

   - **Nombre**

     Nombre de la subred. Debe ser único dentro de la lista global de subredes. Si introduce el nombre que ya existe en la lista, se añadirá un índice, por ejemplo: ~~ 1, ~~ 2.

   - **Descripción**

     La descripción puede contener información adicional sobre la sucursal que tiene esta subred. Este texto aparecerá en todas las listas donde esté presente esta subred, por ejemplo, en la lista de reglas de limitación de tráfico.

     Este campo no es obligatorio y puede dejarse vacío.
6. Haga clic en **Aceptar**.

La subred aparece en la lista de subredes.

## Ver y modificar las propiedades de subred en la lista global de subredes

Puede ver y modificar las propiedades de las subredes en la lista global de subredes.

*Ver o modificar propiedades de una subred en la lista global de subredes:*

1. En el árbol de la consola, seleccione el nodo del Servidor de administración que necesite.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
3. En la ventana **Propiedades** que se abre, en el panel **Secciones** que verá a la izquierda, seleccione **Lista de subredes globales**.
4. En la lista, seleccione la subred que desee.
5. Haga clic en el botón **Propiedades**.

   Se abre la ventana **Nueva subred**.
6. Si es necesario, cambie la configuración de la subred.
7. Haga clic en **Aceptar**.

Si ha realizado cambios, serán almacenados.

# Uso del Agente de red para Windows, Linux y macOS: comparación

El uso del Agente de red varía según el sistema operativo del dispositivo. Los ajustes de la directiva y del paquete de instalación del Agente de red también difieren según el sistema operativo. La tabla de abajo compara las características del Agente de red y los escenarios de uso disponibles para los sistemas operativos Windows, macOS y Linux.

Comparación de funciones del Agente de red

| Función del Agente de red | Windows | Linux | macOS |
|---|---|---|---|
| Instalación | | | |
| Generación automática del paquete de instalación del Agente de red después de la instalación de Kaspersky Security Center | ✓ | — | — |
| Instalación en modo forzado, usando opciones especiales en la tarea de instalación remota de Kaspersky Security Center | ✓ | ✓ | ✓ |
| Instalación con paquetes independientes generados por Kaspersky Security Center y descargados por los usuarios en sus dispositivos a través de vínculos que se le proporcionan oportunamente | ✓ | ✓ | ✓ |

| Función del Agente de red | Windows | Linux | macOS |
|---|---|---|---|
| Instalación con una imagen clónica del disco duro del administrador, que contenga un sistema operativo y una copia del Agente de red y se haya generado con las herramientas provistas por Kaspersky Security Center para trabajar con imágenes de disco | ✓ | — | — |
| Instalación con una imagen clónica del disco duro del administrador, que contenga un sistema operativo y una copia del Agente de red y se haya generado con herramientas desarrolladas por terceros para trabajar con imágenes de disco | ✓ | ✓ | ✓ |
| Instalación con herramientas de terceros para la instalación remota de aplicaciones | ✓ | ✓ | ✓ |
| Instalación manual, ejecutando el instalador de la aplicación en los dispositivos | ✓ | ✓ | ✓ |
| Instalación del Agente de red en modo silencioso | ✓ | ✓ | ✓ |
| Conexión manual de un dispositivo cliente al Servidor de administración (utilidad klmover) | ✓ | ✓ | ✓ |
| Instalación automática de actualizaciones y parches para los componentes de Kaspersky Security Center | ✓ | ✓ | — |
| Distribución automática de una clave | ✓ | ✓ | ✓ |
| Sincronización forzada | ✓ | ✓ | ✓ |
| **Punto de distribución** | | | |
| Uso como punto de distribución | ✓ | ✓ | ✓ |
| Designación automática de puntos de distribución | ✓ | ✓<br>Sin utilizar el reconocimiento de ubicación de red (NLA). | ✓<br>Sin utilizar el reconocimiento de ubicación de red (NLA). |
| Sondeo de red | ✓<br>• Sondeo de la red de Windows<br>• Sondeo de intervalos IP<br>• Sondeo del controlador de dominio (Microsoft Active Directory) | ✓<br>• Sondeo de intervalos IP<br>• Sondeo con Zeroconf<br>• Sondeo del controlador de dominio (Microsoft Active Directory, Samba 4 Active Directory) | — |
| Ejecución del servicio de proxy de KSN en un punto de distribución | ✓ | ✓ | — |
| Descarga de actualizaciones a través de los servidores de actualización de Kaspersky a los repositorios de los puntos de distribución que distribuyen actualizaciones a los dispositivos administrados | ✓ | ✓ | —<br>(Si hay uno o más dispositivos con Linux o macOS en el alcance de la tarea "Descargar actualizaciones en los repositorios de los puntos de distribución", la tarea terminará con el estado "Error" aunque se complete sin errores en todos los dispositivos con Windows). |

| Función del Agente de red | Windows | Linux | macOS |
|---|---|---|---|
| Insertar (push) instalación de aplicaciones | ✓ | Restringido: no es posible realizar una instalación remota en dispositivos Windows mediante el uso de puntos de distribución Linux. | Restringido: no es posible realizar una instalación remota en dispositivos Windows mediante el uso de puntos de distribución macOS. |
| Uso como servidor push | ✓ | ✓ | — |
| **Administración de aplicaciones de terceros** | | | |
| Instalación remota de aplicaciones en dispositivos | ✓ | — | ✓<br>Consulte el siguiente artículo para obtener más detalles: Instalación remota de aplicaciones en dispositivos macOS. |
| Instalación de actualizaciones de software | ✓ | — | — |
| Configuración de actualizaciones del sistema operativo en una directiva del Agente de red | ✓ | — | — |
| Consulta de información sobre las vulnerabilidades de software | ✓ | — | — |
| Análisis de aplicaciones en busca de vulnerabilidades | ✓ | — | — |
| Inventariado del software instalado en los dispositivos | ✓ | ✓ | — |
| **Máquinas virtuales** | | | |
| Instalación del Agente de red en una máquina virtual | ✓ | ✓ | ✓ |
| Optimización de la configuración para infraestructura de escritorio virtual (VDI) | ✓ | ✓ | ✓ |
| Compatibilidad con máquinas virtuales dinámicas | ✓ | ✓ | ✓ |
| **Otro** | | | |
| Acciones de auditoría en dispositivos cliente remotos mediante Windows Desktop Sharing | ✓ | — | — |
| Supervisión del estado de protección antivirus | ✓ | ✓ | ✓ |
| Administración del reinicio de los dispositivos | ✓ | — | — |
| Compatibilidad con las reversiones de estado en los sistemas de archivos | ✓ | ✓ | ✓ |
| Uso del Agente de red como puerta de enlace de conexión | ✓ | ✓ | ✓ |
| Administrador de conexiones | ✓ | ✓ | ✓ |
| Cambio del Servidor de administración al que está conectado el Agente de red (de forma automática, según la ubicación de red) | ✓ | — | ✓ |
| Comprobación de la conexión entre un dispositivo administrado y el Servidor de administración (utilidad klnagchk) | ✓ | ✓ | ✓ |
| Conexión remota al escritorio de un dispositivo cliente | ✓ | — | ✓<br>A través del sistema VNC (siglas de "Virtual Network Computing", computación virtual en red) |

| Función del Agente de red | Windows | Linux | macOS |
| --- | --- | --- | --- |
| Descarga de un paquete de instalación independiente a través del Asistente de migración | ✓ | ✓ | ✓ |
| Sondeo con Zeroconf | — | ✓ | — |
| Ver información sobre el hardware de los dispositivos cliente | ✓ | ✓<br><br>La información sobre el hardware de los dispositivos Linux enviada al Servidor de administración por el Agente de red instalado en estos dispositivos se limita a la información especificada en la descripción de la configuración del dispositivo administrado para la Consola de administración y Kaspersky Security Center Web Console. | ✓<br><br>La información sobre el hardware de los dispositivos macOS enviada al Servidor de administración por el Agente de red instalado en estos dispositivos se limita a la información especificada en la descripción de la configuración del dispositivo administrado para la Consola de administración y Kaspersky Security Center Web Console. |

# Kaspersky Security Center Web Console

Kaspersky Security Center Web Console (de aquí en adelante, también denominada Kaspersky Security Center Web Console) es una aplicación web diseñada para administrar el estado del sistema de seguridad de la red protegida por las aplicaciones de Kaspersky.

El uso de la aplicación le permite hacer lo siguiente:

- Administrar el estado del sistema de seguridad de su organización.
- Instalar aplicaciones de Kaspersky en dispositivos de su red y administrar las aplicaciones instaladas.
- Administrar directivas creadas para sus dispositivos conectados en red.
- Administrar de cuentas de usuario.
- Gestione tareas para aplicaciones instaladas en sus dispositivos de red.
- Ver los informes sobre el estado del sistema de seguridad.
- Administrar la entrega de informes a los administradores del sistema y otros expertos en TI.

Para obtener información sobre los requisitos de hardware y software, consulte Requisitos de Web Console.

Kaspersky Security Center Web Console proporciona una interfaz web que garantiza la interacción entre su dispositivo y el Servidor de administración a través de un navegador. El Servidor de administración es una aplicación diseñada para administrar las aplicaciones Kaspersky instaladas en los dispositivos de red. El Servidor de administración se conecta a los dispositivos de su red a través de canales protegidos por el protocolo SSL. Cuando se conecta a Kaspersky Security Center Web Console con su navegador, el navegador establece una conexión con el Servidor de Kaspersky Security Center Web Console.

Kaspersky Security Center Web Console funciona de la siguiente manera:

1. Utilice un navegador para conectarse a Kaspersky Security Center Web Console, donde se muestran la interfaz del portal web.
2. Utilice los controles del portal web para elegir un comando que desee ejecutar. Kaspersky Security Center Web Console realiza las siguientes operaciones:
    - Si selecciona un comando utilizado para recibir información (por ejemplo, para ver una lista de dispositivos), Kaspersky Security Center Web Console genera una solicitud de información para el Servidor de administración, recibe los datos necesarios y los envía al navegador en un formato de fácil visualización.
    - Si ha seleccionado un comando utilizado para la administración (por ejemplo, instalación remota de una aplicación), Kaspersky Security Center Web Console recibe el comando desde el navegador y lo envía al Servidor de administración. A continuación, la aplicación recibe el resultado del Servidor de administración y lo envía al navegador en un formato de fácil visualización.

Kaspersky Security Center Web Console es una aplicación multilingüe. Puede cambiar el idioma de la interfaz en cualquier momento, sin necesidad de cerrar y volver a abrir la aplicación. Al instalar Kaspersky Security Center Web Console junto con Kaspersky Security Center, Kaspersky Security Center Web Console tiene el mismo idioma de interfaz que el archivo de instalación. Cuando solo instala Kaspersky Security Center Web Console, la aplicación tiene el mismo idioma de la interfaz que su sistema operativo. Si Kaspersky Security Center Web Console no admite el idioma del archivo de instalación o del sistema operativo, el idioma inglés se configura de forma predeterminada.

La Administración de dispositivos móviles no es compatible con Kaspersky Security Center Web Console. Sin embargo, si agregó dispositivos móviles a un grupo de administración utilizando Microsoft Management Console, estos dispositivos también se muestran en Kaspersky Security Center Web Console.

# Diagrama de despliegue del Servidor de administración de Kaspersky Security Center y Kaspersky Security Center Web Console

La siguiente figura muestra el diagrama de despliegue del Servidor de administración de Kaspersky Security Center y Kaspersky Security Center Web Console.

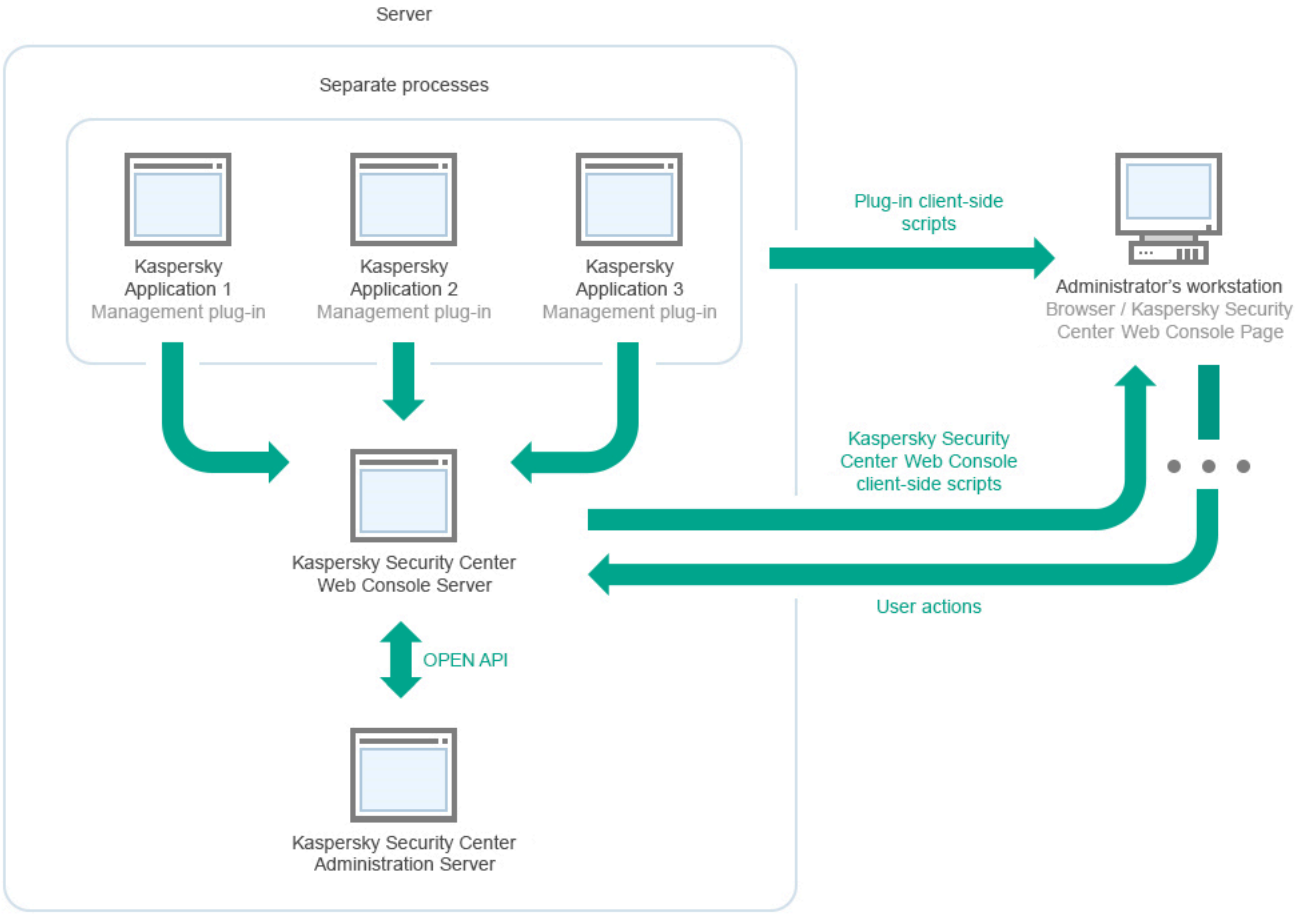



Diagrama de despliegue del Servidor de administración de Kaspersky Security Center y Kaspersky Security Center Web Console

Los complementos de administración para las aplicaciones de Kaspersky instaladas en los dispositivos protegidos (un complemento por aplicación) se despliegan junto con el Servidor de Kaspersky Security Center Web Console.

Como administrador, accede a Kaspersky Security Center Web Console usando un navegador en su estación de trabajo.

Cuando usted realiza acciones específicas en Kaspersky Security Center Web Console, el Servidor de Kaspersky Security Center Web Console se comunica con el Servidor de administración de Kaspersky Security Center a través de OpenAPI. El Servidor de Kaspersky Security Center Web Console solicita la información necesaria al Servidor de administración de Kaspersky Security Center y muestra los resultados de las operaciones en Kaspersky Security Center Web Console.

# Puertos usados por Kaspersky Security Center Web Console

El dispositivo en el que instale el Servidor de Kaspersky Security Center Web Console (también denominado Kaspersky Security Center Web Console) debe tener abiertos los puertos que se indican en la siguiente tabla.

Puertos usados por Kaspersky Security Center Web Console

| Número de puerto | Nombre del servicio | Protocolo | Objetivo del puerto | Alcance |
|---|---|---|---|---|
| 2001 | Kaspersky Security Center Product Plugins Server | HTTPS | Puerto de la API. Se utiliza con los procesos del complemento de administración para recibir solicitudes del Servicio de administración de Kaspersky Security Center Web Console. | Ejecución de procesos node.exe de complementos de administración |
| 1329, 2003 | Servicio de administración de Kaspersky Security Center Web Console | HTTPS | Puertos de la API. Se utilizan para recibir solicitudes del Servicio de administración de Kaspersky Security Center Web Console que se ejecuta en el mismo dispositivo. | Actualización de los componentes de Kaspersky Security Center Web Console |
| 2005 | Kaspersky Security Center Web Console | HTTPS | Puerto de la API. Se utiliza para recibir las solicitudes del Servicio de administración de Kaspersky Security Center Web Console que se ejecuta en el mismo dispositivo. | Ejecución de los procesos node.exe de Kaspersky Security Center Web Console |
| 3333 | Servicio de Kaspersky OSMP KAS | HTTPS | Puerto de endpoint de autorización OAuth2.0 | Identity and Access Manager |
| 4004 | Servicio de Kaspersky OSMP Facade | HTTPS | Puerto del proveedor de identidad OAuth2.0 | Identity and Access Manager |
| 4444 | Servicio de Kaspersky OSMP KAS | HTTPS | Puerto de endpoint de introspección de token OAuth2.0 | Identity and Access Manager |
| 8200 | — | HTTP | Puerto de la API. Se utiliza para generar certificados con HashiCorp Vault (para más información, visite el sitio web de HashiCorp Vault ). | Instalación de Kaspersky Security Center Web Console y actualización de los componentes de Kaspersky Security Center Web Console |
| 4150, 4151, 4152 | Cola de mensajes de Kaspersky Security Center Web Console | HTTPS | Puertos de la API del agente de mensajes utilizados para la comunicación entre los procesos de Kaspersky Security Center Web Console y los complementos de administración | Interacción entre Kaspersky Security Center Web Console y los complementos de administración |

La siguiente tabla enumera los puertos que no tienen que estar abiertos en el dispositivo donde está instalado el servidor de Kaspersky Security Center Web Console. Sin embargo, Kaspersky Security Center Web Console utiliza estos puertos para Identity and Access Manager.

Puertos utilizados por Kaspersky Security Center Web Console para Identity and Access Manager

| Número de puerto | Nombre del servicio | Protocolo | Objetivo del puerto | Alcance |
|---|---|---|---|---|
| 4445 | Servicio de Kaspersky OSMP KAS | HTTPS | Puerto principal de Identity and Access Manager que recibe la configuración de Kaspersky Security Center Web Console para el puerto de endpoint de autorización OAuth2.0 (para obtener más información sobre OAuth 2.0, consulte el sitio web de OAuth ) | Identity and Access Manager |
| 2444 | Servicio de Kaspersky OSMP Facade | HTTPS | Puerto para la configuración de Identity and Access Manager | Identity and Access Manager |
| 2445 | Servicio de Kaspersky OSMP Facade | HTTPS | Puerto para la conexión del servicio de Kaspersky OSMP KAS al servicio de Kaspersky OSMP Facade | Identity and Access Manager |

# Interfaz de Kaspersky Security Center Web Console

Kaspersky Security Center se administra a través de la interfaz de Kaspersky Security Center Web Console.

La ventana de Kaspersky Security Center Web Console contiene los siguientes elementos:

- un menú principal, en la parte izquierda de la ventana
- un área de trabajo, en la parte derecha de la ventana

## Menú principal

El menú principal contiene estas secciones:

- **Servidor de administración**. Muestra el nombre del Servidor de administración al que se está conectado. Haga clic en el icono de configuración ( ) para abrir las propiedades del Servidor de administración.
- **Supervisión e informes**. Brinda una visión general de la infraestructura, los estados de protección e información estadística.
- **Activos (dispositivos)**. Contiene herramientas para los activos, así como tareas y directivas para las aplicaciones de Kaspersky.
- **Usuarios y roles**. Permite administrar los usuarios y sus roles, configurar derechos de usuario mediante la asignación de roles a los usuarios y asociar perfiles de directivas con roles.
- **Operaciones**. Contiene una variedad de operaciones, incluidas la licencia de aplicaciones, la visualización y administración de unidades cifradas y eventos de cifrado, y la administración de aplicaciones de terceros. También brinda acceso a los repositorios de aplicaciones.
- **Descubrimiento y despliegue**. Permite sondear la red para detectar dispositivos cliente y organizar los dispositivos en grupos de administración de forma manual o automática. Esta sección también contiene el asistente de inicio rápido y el asistente de despliegue de la protección.
- **Marketplace**. Contiene información sobre toda la gama de soluciones empresariales de Kaspersky; permite seleccionar las que se necesitan y comprarlas en el sitio web de Kaspersky.

- **Configuración**. Permite crear una copia de seguridad del estado de un complemento web para que sea posible restaurar el estado guardado en otro momento. Contiene también los ajustes personales del usuario vinculados al aspecto de la interfaz, como el idioma o el tema.

- **Menú de su cuenta**. Contiene un vínculo a la Ayuda de Kaspersky Security Center. También le permite cerrar sesión en Kaspersky Security Center y ver la versión de Kaspersky Security Center Web Console y la lista de complementos web de administración instalados.

### Área de trabajo

El área de trabajo muestra la información que elige ver en las secciones de la ventana de la interfaz de Kaspersky Security Center Web Console. También contiene elementos de control que puede usar para configurar cómo se muestra la información.

# Anclar y desanclar secciones del menú principal

Puede anclar sus secciones favoritas de Kaspersky Security Center Web Console para acceder a ellas rápidamente desde la sección **Anclado** del menú principal.

> Si no hay ningún elemento anclado, la sección **Anclado** no se muestra en el menú principal.

Únicamente se pueden anclar las secciones que muestran alguna página. Por ejemplo, si va a **Activos (dispositivos)** → **Dispositivos administrados**, abre una página con una tabla de dispositivos; esto significa que la sección **Dispositivos administrados** puede anclarse. Si se muestra una ventana o no se muestra ningún elemento después de seleccionar una sección en el menú principal, esa sección no se puede anclar.

*Para anclar una sección:*

1. En el menú principal, coloque el cursor del mouse sobre la sección que desee anclar.

   Se muestra el icono de anclar (📌).

2. Haga clic en el icono de anclar (📌).

   Se ancla la sección y se la muestra en la sección **Anclado**.

También puede desanclar los elementos que ya no considere favoritos.

*Para desanclar una sección:*

1. En el menú principal, vaya a la sección **Anclado**.

2. Pase el cursor del ratón sobre la sección que desea desanclar y haga clic en el icono de desanclar (📌).

   La sección se elimina de las favoritas.

# Escenario: Instalación y configuración inicial de Kaspersky Security Center Web Console

Este escenario describe cómo instalar el Servidor de administración de Kaspersky Security Center y la Kaspersky Security Center Web Console, realizar la configuración inicial del Servidor de administración utilizando el Asistente de inicio rápido e instalar las aplicaciones de Kaspersky en los dispositivos administrados utilizando el Asistente de despliegue de la protección.

La instalación y la configuración inicial de Kaspersky Security Center Web Console se dividen en etapas:

1. **Instalación de un sistema de gestión de bases de datos (DBMS)**

   Instale el DBMS que utilizará Kaspersky Security Center o utilice uno existente.

   **Para obtener información sobre cómo instalar el DBMS seleccionado, consulte su documentación.**

2. **Instalación del Servidor de administración, la Consola de administración y el Agente de red**

   La Consola de administración y la versión del servidor del Agente de red se instalan junto con el Servidor de administración.

   Durante la instalación del Servidor de administración de Kaspersky Security Center, especifique si desea instalar Kaspersky Security Center Web Console en el mismo dispositivo. Si elige instalar ambos componentes en el mismo dispositivo, no tiene que instalar Kaspersky Security Center Web Console por separado, ya que se instala automáticamente. Si desea instalar Kaspersky Security Center Web Console en un dispositivo diferente, después de instalar el Servidor de administración de Kaspersky Security Center, proceda a instalar la Kaspersky Security Center Web Console.

3. **Instalación de Kaspersky Security Center Web Console**

   Si no optó, en el paso anterior, por instalar Kaspersky Security Center Web Console junto con el Servidor de administración de Kaspersky Security Center, instale Kaspersky Security Center Web Console por separado. Puede instalar Kaspersky Security Center Web Console en el mismo dispositivo en el que haya instalado el Servidor de administración o en un dispositivo diferente.

4. **Realizar la configuración inicial**

   Cuando termine de instalar el Servidor de administración y se conecte a él por primera vez, se ejecutará automáticamente el asistente de inicio rápido. Realice la configuración inicial del Servidor de administración según los requisitos existentes. Durante la etapa de configuración inicial, el asistente usará los ajustes predeterminados para crear las directivas y tareas necesarias para desplegar la protección. Estos ajustes podrían no ser los ideales para su organización. Puede cambiar la configuración de directivas y tareas si es necesario.

5. **Licencias de Kaspersky Security Center (opcional)**

   Para utilizar Kaspersky Security Center con las funciones básicas de la Consola de administración no se requiere una licencia. Necesita una licencia comercial si desea usar una o varias de las funciones adicionales, que incluyen Administración de vulnerabilidades y parches, Administración de dispositivos móviles e Integración con los sistemas SIEM. Puede agregar archivo de clave o un código de activación para estas funciones en el paso correspondiente del Asistente de inicio rápido o manualmente.

6. **Detección de dispositivos de red**

Esta etapa puede completarse con el Asistente de inicio rápido. También puede descubrir los dispositivos manualmente. Kaspersky Security Center recibe las direcciones y nombres de todos los dispositivos detectados en la red. Puede usar a continuación Kaspersky Security Center para instalar Aplicaciones de Kaspersky y software desde otros proveedores en los dispositivos detectados. Kaspersky Security Center realiza un descubrimiento de dispositivos periódicamente, lo que significa que si aparece alguna instancia nueva en la red, se la detectará automáticamente.

7. **Organización de dispositivos en grupos de administración**

   Esta etapa puede completarse con el Asistente de inicio rápido, pero los dispositivos detectados también se pueden organizar en grupos manualmente.

8. **Instalación del Agente de red y aplicaciones de seguridad en dispositivos en red**

   La instalación de la protección en una red empresarial implica la instalación del Agente de red y de aplicaciones de seguridad (por ejemplo, Kaspersky Endpoint Security para Windows) en dispositivos que el Servidor de administración ha detectado durante el descubrimiento de dispositivos.

   Para instalar las aplicaciones de forma remota, ejecute el Asistente de despliegue de la protección.

   Las aplicaciones de seguridad se encargan de proteger a los dispositivos contra virus y otros programas riesgosos. El Agente de red garantiza la comunicación entre el dispositivo y el Servidor de administración. La configuración de Agente de red se ajusta automáticamente de forma predeterminada.

   Antes de iniciar la instalación de Agente de red y las aplicaciones de seguridad en dispositivos en red, asegúrese de que estos dispositivos estén accesibles (encendidos).

9. **Despliegue de claves de licencia a los dispositivos cliente**

   Despliegue claves de licencia a los dispositivos cliente para activar las aplicaciones de seguridad administradas en esos dispositivos.

10. **Instalación de Kaspersky Security for Mobile (opcional)**

    Si planea administrar dispositivos móviles corporativos, siga las instrucciones que se brindan en la Ayuda de Kaspersky Security para dispositivos móviles. Allí encontrará información sobre el despliegue de Kaspersky Endpoint Security para Android.

11. **Configuración de directivas de la aplicación de Kaspersky**

    Para aplicar diferentes configuraciones de aplicaciones a diferentes dispositivos, puede usar la administración de seguridad centrada en el dispositivo, la administración de seguridad centrada en el usuario y/o una combinación de estos dos enfoques. La administración de la seguridad centrada en el dispositivo se puede implementar mediante el uso de directivas y tareas. Solo puede aplicar tareas a aquellos dispositivos que cumplan condiciones específicas. Para establecer las condiciones para filtrar dispositivos, use selecciones de dispositivos y etiquetas.

12. **Supervisión del estado de protección de la red**

    Puede supervisar su red utilizando widgets en el panel, generar informes desde las aplicaciones de Kaspersky, configurar y ver selecciones de eventos recibidos de las aplicaciones en los dispositivos administrados y ver listas de notificaciones.

# Instalación

Esta sección describe la instalación de Kaspersky Security Center y Kaspersky Security Center Web Console.

# Instalar Kaspersky Security Center (Instalación estándar)

Este procedimiento describe cómo instalar Kaspersky Security Center. Antes de la instalación, debe instalar un sistema de administración de bases de datos.

*Instalar Kaspersky Security Center:*

1. En una cuenta con privilegios administrativos, ejecute el archivo ejecutable ksc_<número de compilación>_full_<idioma de localización>.exe
2. En la ventana de selección de la aplicación que se abre, haga clic en **Instalar Kaspersky Security Center**.

   Se inicia el Asistente de instalación del Servidor de administración de Kaspersky Security Center.
3. Comenzando con la página de bienvenida, continúe con el Asistente usando el botón **Siguiente**.
4. Si Microsoft.NET Framework no se instala, instálelo.
5. Acepte los términos del Contrato de licencia y la Política de privacidad.
6. Seleccione el tipo de instalación. Para fines de evaluación, le recomendamos que mantenga el valor **Estándar** predeterminado.
7. Si desea instalar Kaspersky Security Center Web Console en el mismo dispositivo, seleccione la casilla de verificación **Instalar Kaspersky Security Center Web Console**.

   Si desactiva la casilla de verificación, puede instalar más adelante Kaspersky Security Center Web Console por separado en el mismo o en otro dispositivo.
8. Seleccione el tamaño de su red. Para fines de evaluación, le recomendamos que mantenga el valor **Menos de 100 dispositivos en la red** predeterminado.
9. Seleccione el tipo del servidor de la base de datos que instaló antes.
10. Especifique los parámetros de conexión para el servidor de la base de datos que instaló antes.
11. Especifique los parámetros de autenticación para el servidor de la base de datos que instaló antes.
12. Haga clic en el botón **Instalar** para iniciar la instalación.
13. Una vez que la instalación finalice correctamente, elija si desea iniciar la Consola de administración inmediatamente después de cerrar el Asistente.

    Si elige abrir Kaspersky Security Center Web Console, se abrirá la pantalla de inicio de sesión. Después, podrá realizar la configuración inicial del Servidor de administración utilizando el Asistente de inicio rápido.

    Puede abrir Kaspersky Security Center Web Console solo si ya está instalado. No puede abrir la Kaspersky Security Center Web Console si no la instaló durante la instalación de Kaspersky Security Center o por separado.
14. En la ventana de la Consola de administración que se abre, haga clic en el Servidor de administración instalado.
15. En la ventana del certificado del Servidor de administración que se abre, haga clic en el botón **Sí** para continuar.

El Asistente de inicio rápido del Servidor de administración se inicia si no lo ejecutó en la Consola de administración basada en la web.

### Resolución de problemas

Si la ventana del certificado del Servidor de administración no se abre y se muestran los errores de conexión, intente lo siguiente:

1. En Windows, abra **Servicios** (**Panel de control** → **Herramientas administrativas** → **Servicios**). Compruebe que se estén ejecutando los servicios del Agente de red de Kaspersky Security Center y del Servidor de administración de Kaspersky Security Center.

2. En Windows, abra el **Visor de eventos** (**Panel de control** → **Herramientas administrativas** → **Visor de eventos**) y luego seleccione **Registros de aplicaciones y servicios** → **Registro de eventos de Kaspersky**. Asegúrese de que el registro no contenga errores y contenga eventos como **Servidor de administración <número de versión> se está ejecutando**.

## Instalación de Kaspersky Security Center Web Console

Esta sección describe cómo instalar el Servidor de Kaspersky Security Center Web Console (también conocido como Kaspersky Security Center Web Console) por separado. Antes de la instalación, debe instalar un DBMS y el Servidor de administración de Kaspersky Security Center. Kaspersky Security Center Web Console se puede instalar en el mismo dispositivo en el que está instalado Kaspersky Security Center, o en uno diferente.

*Para instalar Kaspersky Security Center Web Console:*

1. Utilizando una cuenta con privilegios de administrador, ejecute el archivo de instalación ksc-web-console-<número de versión>.<número de compilación>.exe.

   Esto inicia el asistente de instalación.

2. Seleccione un idioma para el Asistente de instalación.

3. En la ventana de bienvenida, haga clic en **Siguiente**.

4. En la ventana **Contrato de licencia**, lea y acepte las condiciones del Contrato de licencia de usuario final. La instalación continúa después de aceptar el EULA, de lo contrario, el botón **Siguiente** no estará disponible.

5. En la ventana **Carpeta de destino** seleccione una carpeta donde Kaspersky Security Center Web Console se instalará (de forma predeterminada, %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console). Si la carpeta no existe, se crea automáticamente durante la instalación.

   Es posible cambiar la carpeta de destino usando el botón **Examinar**.

6. En la ventana **Configuración de conexión de Kaspersky Security Center Web Console**, especifique la siguiente información:

   - La dirección de Kaspersky Security Center Web Console (de forma predeterminada, 127.0.0.1).
   - El puerto que utilizará Kaspersky Security Center Web Console para las conexiones entrantes; es decir, el puerto que permite el acceso a Kaspersky Security Center Web Console desde un navegador (de forma predeterminada, 8080).

   Le recomendamos que deje la dirección y el número de puerto como están.

   Si lo desea, puede hacer clic en **Probar** para asegurarse de que el puerto seleccionado esté disponible.

   Si desea habilitar el registro de las actividades de Kaspersky Security Center Web Console, seleccione la opción adecuada. Si no selecciona esta opción, los archivos de registro de Kaspersky Security Center Web Console no se crearán.

7. En la ventana **Configuración de cuentas**, especifique los nombres de la cuenta y contraseñas.

   Le recomendamos que utilice cuentas predeterminadas.

8. En la ventana **Certificado de cliente**, seleccione uno de lo siguiente:

   - **Generar nuevo certificado**. Se recomienda esta opción si no tiene un certificado de navegador.
   - **Elegir certificado existente**. Puede seleccionar esta opción si ya tiene un certificado de navegador; en este caso, especifique su ruta.
   - Si decide generar un nuevo certificado, cuando abra Kaspersky Security Center Web Console, el navegador puede informarle que la conexión a Kaspersky Security Center Web Console no es privada y que el certificado de Kaspersky Security Center Web Console no es válido. La advertencia se muestra porque Kaspersky Security Center Web Console utiliza un certificado autofirmado, generado automáticamente por Kaspersky Security Center. Para eliminar esta advertencia, cree un certificado que sea de confianza en su infraestructura y que cumpla con los requisitos para certificados personalizados. A continuación, seleccione la opción **Elegir certificado existente** en la ventana **Certificado de cliente** y especifique la ruta a su certificado personalizado.

   Los certificados en el formato PFX no son compatibles con Kaspersky Security Center Web Console. Para utilizar dicho certificado, primero debe convertirlo al formato PEM compatible utilizando una utilidad multiplataforma basada en OpenSSL, como OpenSSL para Windows.

9. En la ventana **Servidores de administración de confianza**, asegúrese de que su Servidor de administración esté en la lista y haga clic en **Siguiente** para ir a la última ventana del instalador.

   Si necesita agregar un nuevo Servidor de administración a la lista, haga clic en el botón **Agregar**. En la ventana abierta, especifique las propiedades de un nuevo Servidor de administración de confianza:

   - **Nombre del Servidor de administración**

     El nombre del Servidor de administración que aparecerá en la ventana de inicio de sesión de Kaspersky Security Center Web Console.

   - **Dirección del Servidor de administración**

     La dirección IP del dispositivo donde instala el Servidor de Administración.

   - **Puerto del Servidor de administración**

     El puerto de OpenAPI que Kaspersky Security Center Web Console utiliza para conectarse al Servidor de administración (el valor predeterminado es 13299).

   - **Certificado del Servidor de administración**

     El archivo de certificado se almacena en el dispositivo donde está instalado el Servidor de administración. La ruta predeterminada al certificado del Servidor de administración:

     - Para Windows: %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
     - Para Linux: /var/opt/kaspersky/klnagent_srv/1093/cert/

     Si instala Kaspersky Security Center Web Console en el mismo dispositivo donde está instalado el Servidor de administración, use una de las rutas indicadas anteriormente. De lo contrario, copie el archivo del certificado del dispositivo donde está instalado el Servidor de administración al dispositivo donde instaló Kaspersky Security Center Web Console y luego especifique la ruta local al certificado.

10. En la ventana **Identity and Access Manager (IAM)**, especifique si desea instalar Identity and Access Manager (también conocido como IAM). Si elige instalar Identity and Access Manager, especifique los siguientes números de puerto:

    - **Puerto de administrador KAS**. De forma predeterminada, el puerto 4445 se utiliza para recibir la configuración de Kaspersky Security Center Web Console para el puerto de endpoint de autorización OAuth2.0.
    - **Puerto de Facade**. De forma predeterminada, el puerto 2444 se utiliza para la configuración de Identity and Access Manager.
    - **Puerto de interacción Facade**. De forma predeterminada, el puerto 2445 se utiliza para la conexión de Kaspersky OSMP KAS Service con Kaspersky OSMP Facade Service.

    Si lo desea, puede cambiar los números de puerto predeterminados. No podrá cambiarlos en el futuro a través de Kaspersky Security Center Web Console.

11. En la última ventana en el instalador, haga clic en **Instalar** para comenzar la instalación.

Una vez que la instalación se complete con éxito, aparecerá un acceso directo en su escritorio, y puede iniciar sesión en Kaspersky Security Center Web Console.

El Asistente de inicio rápido del Servidor de administración se inicia si no lo ejecutó en la Consola de administración basada en Microsoft Management Console.

### Resolución de problemas

*Si Kaspersky Security Center Web Console no se muestra en su navegador cuando escribe la URL, intente lo siguiente:*

1. Compruebe que haya especificado el nombre de host o la dirección IP correctos del dispositivo en el que está instalada Kaspersky Security Center Web Console.
2. Compruebe que el dispositivo que desea operar tenga acceso al dispositivo en el que está instalada Kaspersky Security Center Web Console.
3. Verifique que la configuración del firewall en el dispositivo en el que está instalado Kaspersky Security Center Web Console permita conexiones entrantes a través del puerto 8080 y para la aplicación node.exe.
4. En Windows, abra **Servicios**. Compruebe que el servicio de Kaspersky Security Center Web Console se esté ejecutando.
5. Compruebe que puede acceder a Kaspersky Security Center mediante la Consola de administración.
6. En Windows, abra el **Visor del evento**, y luego seleccione **Aplicaciones y registros de servicios** → **Registro de eventos de Kaspersky**. Asegúrese que el registro no contenga errores.

# Instalar Kaspersky Security Center Web Console conectado al Servidor de administración instalado en nodos del clúster de conmutación por error de Kaspersky

En esta sección, se describe cómo instalar el Servidor de Kaspersky Security Center Web Console (en adelante, también denominado Kaspersky Security Center Web Console), que se conecta al Servidor de administración instalado en los nodos del clúster de conmutación por error de Kaspersky Security Center o en los nodos del clúster de conmutación por error de Windows Server. Antes de instalar Kaspersky Security Center Web Console, instale un DBMS y un Servidor de administración de Kaspersky Security Center en nodos del clúster de conmutación por error de Kaspersky Security Center o en nodos del clúster de conmutación por error de Windows Server.

Si utiliza un clúster de conmutación por error de Windows Server, no recomendamos instalar Kaspersky Security Center Web Console en un nodo del clúster de conmutación por error. Si el nodo sufriera un problema de funcionamiento, se perdería el acceso al Servidor de administración.

*Para instalar Kaspersky Security Center Web Console que se conecta a Kaspersky Security Center instalado en nodos del clúster de conmutación por error:*

1. Realice los pasos 1 a 8 de la instalación de la Kaspersky Security Center Web Console.

2. En el paso 9, en la ventana **Servidores de administración de confianza**, haga clic en el botón **Agregar** para agregar un clúster de conmutación por error como un Servidor de administración de confianza.

   En la ventana abierta, especifique las siguientes propiedades:

   - **Nombre del Servidor de administración**

     El nombre del clúster que aparecerá en la ventana de inicio de sesión de Kaspersky Security Center Web Console.

   - **Dirección del Servidor de administración**

     Según el tipo de clúster de conmutación por error, especifique la dirección del clúster:

     - **Clúster de conmutación por error de Kaspersky Security Center**. Indique la dirección IP del adaptador de red virtual como dirección del clúster si creó ese adaptador al preparar los nodos del clúster. De lo contrario, ingrese la dirección IP del equilibrador de carga de terceros que esté utilizando.

     - **Clúster de conmutación por error de Windows Server**. Especifique la dirección del clúster que obtuvo al crear el clúster de conmutación por error de Windows Server.

   - **Puerto del Servidor de administración**

     El puerto de OpenAPI que Kaspersky Security Center Web Console utiliza para conectarse al Servidor de administración (el valor predeterminado es 13299).

   - **Certificado del Servidor de administración**

     El certificado del Servidor de administración se encuentra en el almacenamiento de datos compartidos del clúster de conmutación por error de Kaspersky Security Center o el clúster de conmutación por error de Windows Server. La ruta predeterminada al archivo del certificado es <carpeta de datos compartida>\1093\cert\klserver.cer. Copie el archivo del certificado de la carpeta compartida al dispositivo en el que se encuentre instalado Kaspersky Security Center Web Console. Defina la ruta local al certificado del Servidor de administración.

3. Siga con la instalación estándar de Kaspersky Security Center Web Console.

Una vez completada la instalación, aparecerá un acceso directo en el escritorio y podrá iniciar sesión en Kaspersky Security Center Web Console.

# Actualización de Kaspersky Security Center Web Console

Si desea utilizar una versión más reciente de Kaspersky Security Center Web Console sin eliminar la instancia instalada actualmente, puede utilizar el procedimiento de actualización estándar proporcionado en el instalador de Kaspersky Security Center Web Console.

*Para actualizar Kaspersky Security Center Web Console:*

1. Utilizando una cuenta con derechos de administrador, ejecute el archivo de instalación ksc-web-console-<número de versión>-<número de compilación>.exe (el valor de <número de compilación> será un número de compilación de Kaspersky Security Center Web Console posterior al de la copia instalada).

2. En la ventana del Asistente de instalación que se abre, seleccione un idioma y, luego, haga clic en **Sin inconvenientes**.

3. En la ventana de bienvenida, seleccione la opción **Actualizar** y luego haga clic en **Siguiente**.

4. En la ventana **Contrato de licencia**, lea y acepte las condiciones del Contrato de licencia de usuario final. La instalación continúa después de aceptar el EULA; de lo contrario, el botón **Siguiente** no estará disponible.

5. Siga los pasos del Asistente de instalación hasta que finalice la instalación. Al avanzar, también puede modificar la configuración de Kaspersky Security Center Web Console que especificó durante la instalación anterior. Cuando llegue al paso **Preparado para modificar Kaspersky Security Center Web Console**, haga clic en el botón **Actualizar**. Espere hasta que se apliquen las nuevas configuraciones y, en el siguiente paso del Asistente de instalación, haga clic en **Finalizar**. También puede hacer clic en el vínculo **Iniciar Kaspersky Security Center Web Console en su navegador** para iniciar la instancia actualizada de Kaspersky Security Center Web Console inmediatamente.

   La modificación de la configuración de Kaspersky Security Center Web Console durante la actualización solo está disponible en Kaspersky Security Center Web Console versión 12.2 o posterior.

   Se actualiza la instancia de Kaspersky Security Center Web Console.

# Certificados para trabajar con Kaspersky Security Center Web Console

En esta sección, se explica cómo emitir y reemplazar certificados para Kaspersky Security Center 14 Web Console y cómo renovar un certificado para el Servidor de administración si el Servidor interactúa con Kaspersky Security Center 14 Web Console.

## Reemisión del certificado de Kaspersky Security Center Web Console

La mayoría de los navegadores imponen un límite al plazo de validez de un certificado. Para estar dentro de este límite, el plazo de validez del certificado de Kaspersky Security Center Web Console está limitado a 397 días. Puede reemplazar un certificado existente recibido de una autoridad de certificación (CA) emitiendo un nuevo certificado autofirmado manualmente. Como alternativa, puede volver a emitir su certificado de Kaspersky Security Center Web Console caducado.

La reemisión automática del certificado de Kaspersky Security Center Web Console no es compatible. Debe volver a emitir manualmente el certificado caducado.

Si ya usa un certificado autofirmado, también puede volver a emitirlo actualizando Kaspersky Security Center Web Console mediante el procedimiento estándar del instalador (opción **Actualizar**).

Cuando abre Web Console, el navegador le informa que la conexión a Web Console no es privada y que el certificado de Web Console no es válido. La advertencia se muestra porque Web Console utiliza un certificado autofirmado, generado automáticamente por Kaspersky Security Center. Para eliminar esta advertencia o prevenir su aparición, puede realizar una de las acciones siguientes:

- Especifique un certificado personalizado cuando lo vuelva a emitir (opción recomendada). Cree un certificado que sea de confianza en su infraestructura y que cumpla con los requisitos para certificados personalizados.
- Añada el certificado de Web Console a la lista de certificados de navegador de confianza después de volverlo a emitir. Recomendamos que utilice esta opción solo si no puede crear un certificado personalizado.

*Para emitir un nuevo certificado cuando instala Kaspersky Security Center Web Console por primera vez:*

1. Ejecute la instalación de rutina de Kaspersky Security Center Web Console.
2. Cuando llegue al paso **Certificado de cliente** del asistente de instalación, seleccione la opción **Generar nuevo certificado** y, luego, haga clic en el botón **Siguiente**.
3. Continúe con los pasos restantes del asistente de instalación hasta que finalice la instalación.

   Se emite un nuevo certificado para Kaspersky Security Center Web Console con un período de validez de 397 días.

*Para volver a emitir el certificado caducado de Kaspersky Security Center Web Console:*

1. Utilizando una cuenta con derechos de administrador, ejecute el archivo de instalación ksc-web-console-<número de versión>.<número de compilación>.exe.
2. En la ventana del Asistente de instalación que se abre, seleccione un idioma y, luego, haga clic en **Sin inconvenientes**.
3. En la ventana de bienvenida, seleccione la opción **Emitir el certificado nuevamente** y luego haga clic en **Siguiente**.
4. En el siguiente paso, espere hasta que se complete la reconfiguración de Kaspersky Security Center Web Console y luego haga clic en **Finalizar**.

   El certificado de Kaspersky Security Center Web Console se vuelve a emitir por otro período de validez de 397 días.

Si utiliza Identity and Access Manager, también debe volver a emitir todos los certificados TLS para los puertos que utiliza Identity and Access Manager. Kaspersky Security Center Web Console muestra una notificación cuando caduca un certificado. Debe seguir las instrucciones de la notificación.

## Reemplazar el certificado de Kaspersky Security Center Web Console

De forma predeterminada, cuando se instala el Servidor de Kaspersky Security Center Web Console, se genera automáticamente un certificado para acceder a la aplicación con un navegador. Este certificado puede reemplazarse por uno personalizado.

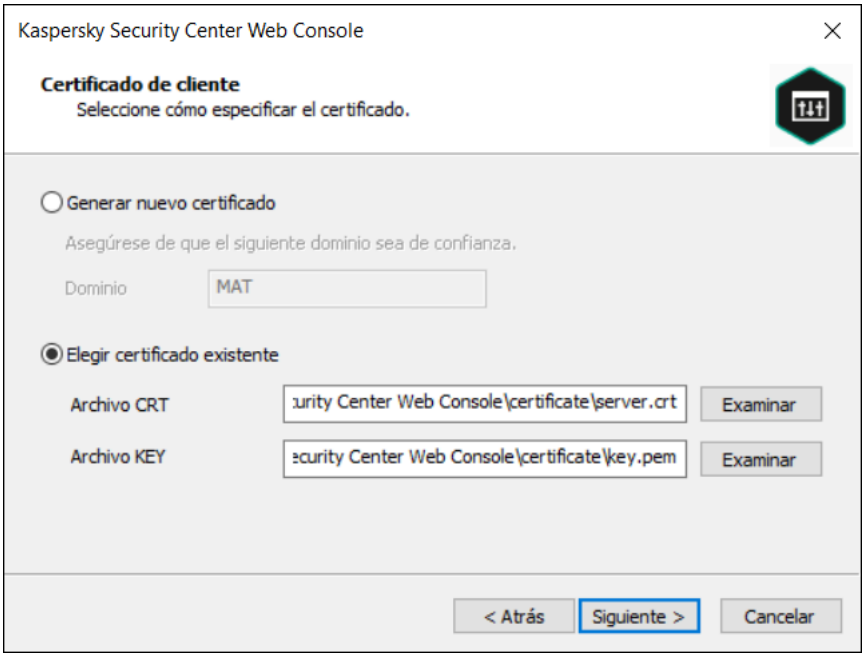
*Para reemplazar el certificado del Servidor de Kaspersky Security Center Web Console por uno personalizado:*

1. En el dispositivo en el que se encuentre instalado el Servidor de Kaspersky Security Center Web Console, ejecute el archivo de instalación ksc-web-console-<número de versión>.<número de compilación>.exe. Utilice para esto una cuenta con privilegios de administrador.

   Esto inicia el asistente de instalación.

2. En la primera página del asistente, seleccione la opción **Actualizar**.

3. En la página **Certificado de cliente**, seleccione la opción **Elija un certificado existente** y especifique la ruta al certificado que desea usar.




Especificar el certificado cliente

4. En la última página del asistente, haga clic en **Modificar** para aplicar la nueva configuración.

5. Cuando la aplicación se haya reconfigurado, haga clic en el botón **Finalizar**.

Kaspersky Security Center Web Console ahora utilizará el nuevo certificado.

## Especificación de certificados para Servidores de administración de confianza en Kaspersky Security Center Web Console

Cuando el certificado del Servidor de administración está por caducar, se lo reemplaza automáticamente con uno nuevo. El certificado del Servidor de administración también se puede reemplazar por uno personalizado. Tenga en cuenta que cada vez que cambie de certificado, deberá especificar el nuevo en la configuración de Kaspersky Security Center Web Console. De lo contrario, Kaspersky Security Center Web Console no podrá conectarse con el Servidor de administración.

*Para especificar la ruta al nuevo certificado del Servidor de administración:*

1. En el dispositivo en el que está instalado el Servidor de administración, copie el archivo del certificado a, por ejemplo, una unidad de almacenamiento masivo.

   De forma predeterminada, el archivo del certificado se almacena en la siguiente carpeta:

   - Para Windows: %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
   - Para Linux: /var/opt/kaspersky/klnagent_srv/1093/cert/

2. En el dispositivo en el que está instalado Kaspersky Security Center Web Console, copie el archivo del certificado a una carpeta local.

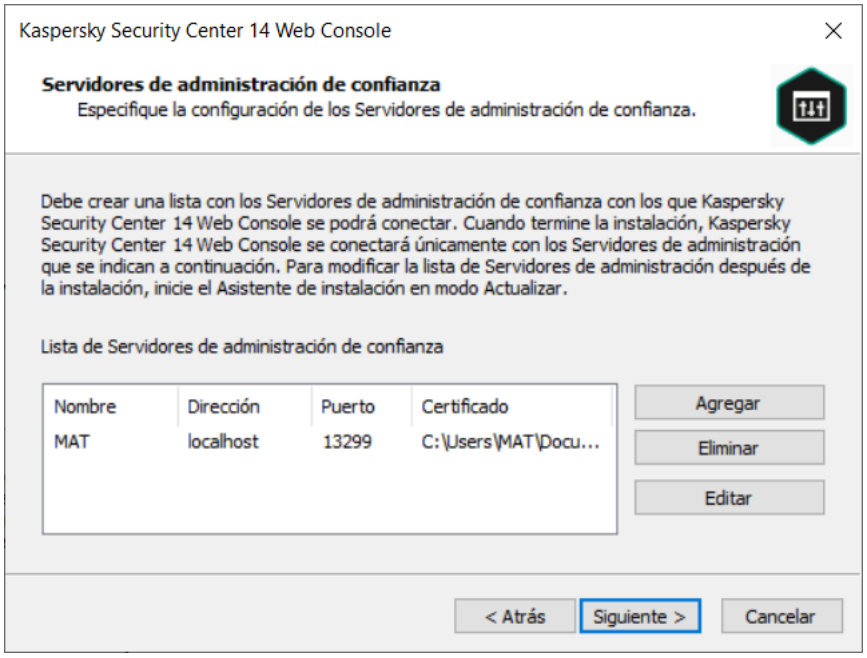
3. Utilizando una cuenta con privilegios de administrador, ejecute el archivo de instalación ksc-web-console-<número de versión>.<número de compilación>.exe.

   Esto inicia el asistente de instalación.

4. En la primera página del asistente, seleccione la opción **Actualizar**.

   Siga las instrucciones del asistente.

5. En la página **Servidores de administración de confianza** del asistente, seleccione el Servidor de administración requerido y haga clic en el botón **Editar**.




Especificar los Servidores de administración de confianza

6. En la ventana **Editar Servidor de administración** que se abre, haga clic en el botón **Examinar**, especifique la ruta al nuevo archivo de certificado y, luego, haga clic en el botón **Actualizar** para aplicar los cambios.

7. En la página **Preparado para modificar Kaspersky Security Center Web Console** del asistente, haga clic en el botón **Actualizar** para iniciar la actualización.

8. Después de que la reconfiguración de la aplicación se complete correctamente, haga clic en el botón **Finalizar**.

9. Inicie sesión en Kaspersky Security Center Web Console.

Kaspersky Security Center Web Console ahora utilizará el nuevo certificado.

# Conversión de un certificado PFX al formato PEM

Si desea utilizar un certificado PFX en Kaspersky Security Center Web Console, primero debe convertirlo al formato PEM. Puede usar para ello cualquier utilidad multiplataforma basada en OpenSSL.

*Para convertir un certificado PFX al formato PEM en el sistema operativo Windows:*

1. En una utilidad multiplataforma basada en OpenSSL, ejecute los siguientes comandos:

   ```
   openssl pkcs12 -in < nombre de archivo .pfx> -clcerts -nokeys -out server.crt
   openssl pkcs12 -in < nombre de archivo .pfx> -nocerts -nodes -out key.pem
   ```

   De este modo, obtendrá una clave pública como archivo .crt y una clave privada como archivo .pem protegido con frases de contraseña.

2. Asegúrese de que los archivos .crt y .pem se generen en la misma carpeta donde se almacena el archivo .pfx.

3. Si el archivo .crt o .pem contiene los "Atributos de la bolsa", elimine esos atributos con cualquier editor de texto conveniente y guarde el archivo.

4. Reinicie el servicio de Windows.

5. Kaspersky Security Center Web Console no permite usar certificados protegidos con una frase de contraseña. Por lo tanto, debe ejecutar el siguiente comando en una utilidad multiplataforma basada en OpenSSL para eliminar una frase de contraseña del archivo .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > No utilice el mismo nombre para los archivos .pem de entrada y salida.

   De este modo, se elimina el cifrado del nuevo archivo .pem. No debe introducir una frase de contraseña para usarlo.

Los archivos .crt y .pem pueden cargarse sin más en el instalador de Kaspersky Security Center Web Console.

*Para convertir un certificado PFX al formato PEM en el sistema operativo Linux:*

1. En una utilidad multiplataforma basada en OpenSSL, ejecute los siguientes comandos:

   ```
   openssl pkcs12 -in < nombre de archivo .pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in < nombre de archivo. pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Asegúrese de que el archivo del certificado y la clave privada se generen en el mismo directorio donde se almacena el archivo .pfx.

3. Kaspersky Security Center Web Console no permite usar certificados protegidos con una frase de contraseña. Por lo tanto, debe ejecutar el siguiente comando en una utilidad multiplataforma basada en OpenSSL para eliminar una frase de contraseña del archivo .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > No utilice el mismo nombre para los archivos .pem de entrada y salida.

   De este modo, se elimina el cifrado del nuevo archivo .pem. No debe introducir una frase de contraseña para usarlo.

Los archivos .crt y .pem pueden cargarse sin más en el instalador de Kaspersky Security Center Web Console.

# Migración desde Kaspersky Security Center Windows

En esta sección, se describe la migración de dispositivos administrados y objetos afines (directivas, tareas, grupos, etiquetas y otros objetos) desde Kaspersky Security Center Windows a:

- Kaspersky Security Center Cloud Console
- Kaspersky Security Center Linux

## Migración a Kaspersky Security Center Cloud Console

Puede realizar la migración de Kaspersky Security Center Web Console a Kaspersky Security Center Cloud Console. Después de eso, obtiene acceso al Servidor de administración y al sistema de administración de bases de datos (DBMS), que están alojados en la infraestructura de Kaspersky. No necesita un servidor físico ni un DBMS; los expertos de Kaspersky se encargan del mantenimiento de ambos.

Puede migrar sus dispositivos administrados con un sistema operativo Windows, Linux o macOS bajo el control de Kaspersky Security Center Cloud Console. Si su red incluye una jerarquía de Servidores de administración, puede guardarla en Kaspersky Security Center Cloud Console. Además, puede transferir lo siguiente:

- Tareas y directivas de aplicaciones administradas
- Tareas globales
- Selecciones de dispositivos personalizados

- Estructura del grupo de administración y dispositivos incluidos
- Etiquetas que se asignaron a los dispositivos en migración

Después de finalizar la migración, puede administrar los dispositivos a través de Kaspersky Security Center Cloud Console. Al mismo tiempo, los objetos transferidos se conservan y el Agente de red se reinstala en todos los dispositivos administrados.

Para obtener información sobre cómo realizar la migración y una lista de los requisitos previos, consulte la *Ayuda de Kaspersky Security Center Cloud Console*.

# Migrar a Kaspersky Next XDR Expert

En este escenario, puede transferir la estructura del grupo de administración, incluidos los dispositivos administrados y otros objetos de grupo (directivas, tareas, tareas globales, etiquetas y selecciones de dispositivos) desde Kaspersky Security Center Windows con la administración de Kaspersky Next XDR Expert.

Limitaciones:

- La migración solo se puede realizar de Kaspersky Security Center 14.2 Windows a Kaspersky Next XDR Expert a partir de la versión 1.0.
- Solo puede realizar este escenario mediante el uso de Kaspersky Security Center Web Console.

## Etapas

El escenario de migración se desarrolla en etapas:

1. **Elija un método de migración**

   Migre a Kaspersky Next XDR Expert a través del Asistente de migración. Los pasos del Asistente de migración dependen de si los Servidores de administración de Kaspersky Security Center Windows y Kaspersky Next XDR Expert están organizados en una jerarquía:

   - Migración con una jerarquía de Servidores de administración

     Elija esta opción si el Servidor de administración de Kaspersky Security Center Windows funciona como servidor secundario del Servidor de administración de Kaspersky Next XDR Expert. Usted administra el proceso de migración y alterna los Servidores dentro de OSMP Console. Si prefiere esta opción, puede organizar los Servidores de administración en una jerarquía para simplificar el procedimiento de migración. Para hacerlo, cree la jerarquía antes de iniciar la migración.

   - Migración con un archivo de exportación (archivo ZIP)

     Elija esta opción si los Servidores de administración de Kaspersky Security Center Windows y Kaspersky Next XDR Expert no están organizados en una jerarquía. El proceso de migración se administra con dos consolas: una instancia para Kaspersky Security Center Windows y OSMP Console. En este caso, utilizará el archivo de exportación que creó y descargó durante la exportación desde Kaspersky Security Center Windows e importará este archivo a Kaspersky Next XDR Expert.

2. **Exportación de datos desde Kaspersky Security Center Windows**

   Abra Kaspersky Security Center Windows y, luego, ejecute el Asistente de migración.

3. **Importar datos a Kaspersky Next XDR Expert**

   Continúe con el Asistente de migración para importar los datos exportados a Kaspersky Next XDR Expert.

Si los servidores están organizados en una jerarquía, la importación se inicia de forma automática después de una exportación exitosa dentro del mismo asistente. Si los Servidores no están organizados en una jerarquía, continúe con el Asistente de migración después de cambiar a Kaspersky Next XDR Expert.

4. **Realice acciones adicionales para transferir objetos y configuraciones de Kaspersky Security Center Windows a Kaspersky Next XDR Expert de forma manual (paso opcional)**

   También es posible transferir los objetos y las configuraciones que no se pueden transferir a través del Asistente de migración. Por ejemplo, también puede hacer lo siguiente:

   - Configurar tareas globales del Servidor de administración
   - Configurar los ajustes de la directiva del Agente de red
   - Crear paquetes de instalación de aplicaciones
   - Crear Servidores virtuales
   - Asignar y configurar puntos de distribución
   - Configurar reglas de movimiento de dispositivos
   - Configurar reglas para etiquetar dispositivos de forma automática
   - Crear categorías de aplicaciones

5. **Mueva los dispositivos administrados importados desde la administración de Kaspersky Next XDR Expert**

   Para completar la migración, mueva los dispositivos administrados importados desde la administración de Kaspersky Next XDR Expert. Puede hacerlo usando uno de los siguientes métodos:

   - A través de la tarea de grupo de Kaspersky Security Center

     Utilice la tarea Cambiar Servidor de administración para cambiar el Servidor de administración a uno diferente en dispositivos cliente específicos.

   - Mediante la utilidad klmover

     Use la utilidad klmover y especifique la configuración de conexión para el nuevo Servidor de administración.

   - Mediante la instalación o reinstalación del Agente de red en los dispositivos administrados

     Cree un nuevo paquete de instalación del Agente de red y especifique la configuración de conexión para el nuevo Servidor de administración en las propiedades del paquete de instalación. Utilice el paquete de instalación para instalar el Agente de red en los dispositivos administrados importados a través de una tarea de instalación remota.

     También puede crear y utilizar un paquete de instalación independiente para instalar el Agente de red de manera local.

6. **Actualice el Agente de red a la versión más reciente**

   Le recomendamos que actualice el Agente de red a la misma versión que OSMP Console.

7. **Asegúrese de que los dispositivos administrados estén visibles en el nuevo Servidor de administración**

   En el Servidor de administración de Kaspersky Next XDR Expert, abra la lista de dispositivos administrados (**Activos (dispositivos)** → **Dispositivos administrados**) y verifique los valores en las columnas **Visible**, **Agente de red instalado** y **Última conexión con el Servidor de administración**.

### Otros métodos de migración de datos

Además del asistente de migración, también puede transferir tareas y directivas específicas:

- Exporte las tareas de Kaspersky Security Center Windows y, a continuación, impórtelas a Kaspersky Next XDR Expert.
- Exporte las directivas de Kaspersky Security Center Windows y, a continuación, impórtelas a Kaspersky Next XDR Expert. Los perfiles de las directivas que seleccione se exportarán e importarán junto con las directivas.

## Migración a Kaspersky Security Center Linux

La migración de Kaspersky Security Center Windows a Kaspersky Security Center Linux está disponible usando el respaldo de los datos del Servidor de administración (con la utilidad klbackup) y el Asistente de migración.

La siguiente tabla le permite comparar las principales características y limitaciones de la migración mediante la copia de seguridad de los datos del Servidor de administración y el Asistente de migración, para decidir qué enfoque es más adecuado para su organización.

Comparación de los enfoques de migración

| Parámetros | Copia de seguridad de los datos del Servidor de administración | Asistente de migración |
|---|---|---|
| Proceso de migración | Crear una copia de seguridad completa de los datos del Servidor de administración de Kaspersky Security Center Windows y restaurarla en un Servidor de administración de Kaspersky Security Center Linux | Seleccionar y exportar los datos del Servidor de administración para la migración, importar estos datos al Servidor de administración de Kaspersky Security Center Linux y cambiar los dispositivos administrados bajo la administración de Kaspersky Security Center Linux |
| Características del método de migración | • Migración de todos los datos del Servidor de administración<br>• Migración de cualquier cantidad de dispositivos administrados<br>• Se utiliza para obtener una copia completa de los datos del Servidor de administración de Kaspersky Security Center Windows y transferirla al Servidor de administración de Kaspersky Security Center Linux | • Migración parcial de los datos del Servidor de administración<br>• La selección de objetos para la migración está disponible<br>• El grupo o subgrupo de administración que se va a migrar no puede contener más de 10 000 dispositivos<br>• Se utiliza para transferir parcialmente los datos del Servidor de administración, incluidos solo los objetos de grupo dentro del alcance de la migración. Los objetos de grupo fuera del alcance de la migración deben restaurarse manualmente |
| Alcance de la migración | Transferencia completa de los datos del Servidor de administración con un número ilimitado de dispositivos administrados | • Estructura de grupos de administración<br>• Dispositivos administrados incluidos en los grupos de administración (**no más de 10 000 dispositivos**)<br>• Etiquetas asignadas a los dispositivos de migración<br>• Tareas globales del Agente de red y aplicaciones administradas (no para el Servidor de administración)<br>• Tareas de grupo del Agente de red y aplicaciones administradas<br>• Directivas de aplicaciones administradas<br>• Plantillas de informes<br>• Roles de usuarios<br>• Usuarios y grupos de seguridad internos<br>• Categorías de aplicaciones personalizadas con contenido agregado manualmente<br>• Selecciones de dispositivos personalizados |

| | | |
|---|---|---|
| Alcance no migrado | — | • Tareas globales del Servidor de administración<br>• Eventos guardados en el Servidor de administración<br>• Repositorio de paquetes de distribución de aplicaciones para instalación remota<br>• Certificado del Servidor de administración<br>• Claves de licencia utilizadas por el Servidor de administración y las aplicaciones administradas<br>• Servidores de administración virtuales<br>• Ajustes de la directiva del Agente de red<br>• Reglas de movimiento de dispositivos<br>• Reglas para etiquetar dispositivos de forma automática<br>• Puntos de distribución<br>• Configuración de la aplicación de Kaspersky guardada en el Servidor de administración |
| Versiones de Kaspersky Security Center que admiten la migración | • Cualquier versión compatible de Kaspersky Security Center Windows<br>• Kaspersky Security Center Linux versión 15.2 o posterior | • Kaspersky Security Center Windows versión 14.2 o posterior<br>• Kaspersky Security Center Linux versión 15 o posterior |
| DBMS entre los que se puede realizar la migración | • Microsoft SQL Server → MySQL, MariaDB<br>• Microsoft SQL Server → PostgreSQL, Postgres Pro (solo para la migración de Kaspersky Security Center Windows versión 14.2 o posterior con el parche instalado a Kaspersky Security Center Linux versión 15.3 o posterior)<br>• MySQL → MySQL, MariaDB<br>• MariaDB → MySQL, MariaDB<br>• PostgreSQL → PostgreSQL<br>Postgres Pro → Postgres Pro (solo para la migración de Kaspersky Security Center Windows versión 15.1 o posterior a Kaspersky Security Center Linux versión 16 o posterior) | Migración entre DBMS compatibles sin limitaciones |

# Migrar a Kaspersky Security Center Linux con una copia de seguridad de los datos del Servidor de administración

Puede utilizar una copia de seguridad para migrar los datos del Servidor de administración de Kaspersky Security Center Windows a Kaspersky Security Center Linux. Antes de la migración, asegúrese de que las funciones de Kaspersky Security Center Windows que necesite estén disponibles en Kaspersky Security Center Linux.

Limitaciones:

- La migración se puede realizar entre los siguientes DBMS:
  - Microsoft SQL Server → MySQL, MariaDB
  - Microsoft SQL Server → PostgreSQL, Postgres Pro
  - MySQL → MySQL, MariaDB
  - MariaDB → MySQL, MariaDB
  - PostgreSQL → PostgreSQL
  - Postgres Pro → Postgres Pro
- La migración de los datos del Servidor de administración almacenados en las bases de datos de Microsoft SQL Server, MySQL o MariaDB a MySQL o MariaDB es compatible para la migración de cualquier versión compatible de Kaspersky Security Center Windows a Kaspersky Security Center Linux versión 15.2 o posterior.
- La migración de los datos del Servidor de administración almacenados en la base de datos de PostgreSQL a PostgreSQL o la base de datos de Postgres Pro a Postgres Pro es compatible con la migración de Kaspersky Security Center Windows versión 15.1 o posterior a Kaspersky Security Center Linux versión 16 o posterior.
- La migración de los datos del Servidor de administración almacenados en las bases de datos de Microsoft SQL Server a PostgreSQL o Postgres Pro es compatible con la migración de Kaspersky Security Center Windows versión 14.2 o posterior a Kaspersky Security Center Linux versión 15.3 o posterior.

  Para admitir la migración a PostgreSQL o Postgres Pro, puede realizar una de las siguientes acciones:
  - Instale el parche 15.1.0.20748-pf2 para el Servidor de administración de Kaspersky Security Center Windows. Comuníquese con el Servicio de soporte técnico de Kaspersky para obtener este parche.
  - Actualice Kaspersky Security Center Windows a la versión 15.1.0.22239.
- Si utiliza MySQL o MariaDB como DBMS para Kaspersky Security Center Windows y Kaspersky Security Center Linux, el parámetro `lower_case_table_names` debe ser el mismo en el DBMS activo y el nuevo.

  Antes de crear una copia de seguridad de los datos, controle el parámetro `lower_case_table_names`. Luego, al instalar MySQL o MariaDB para Kaspersky Security Center Linux, asigne a este parámetro el mismo valor que tenga en Windows.

## Etapas

La migración mediante la copia de seguridad de datos del Servidor de administración se realiza en etapas:

1. **Verificar que tiene la cuenta de usuario interna del administrador con la que puede iniciar sesión en el Servidor de administración**

   La cuenta del administrador se utilizará para iniciar sesión en el Servidor de administración de Kaspersky Security Center Linux. Si no tiene esta cuenta e inició sesión solo con una cuenta local de Windows o con una cuenta de dominio, no podrá iniciar sesión en el Servidor de administración de Kaspersky Security Center Linux después de restaurar la copia de seguridad. El Servidor de administración de Kaspersky Security Center Linux no admite el inicio de sesión con la cuenta local de Windows. Es posible iniciar sesión con la cuenta de dominio, pero puede requerir una configuración adicional del Servidor de administración.

Si no tiene la cuenta de administrador, tendrá que crear esta cuenta después de restaurar la copia de seguridad utilizando la utilidad kladduser.

2. **Creación de una copia de seguridad actualizada de los datos del Servidor de administración de Kaspersky Security Center Windows**

   Según el tipo de DBMS utilizado para Kaspersky Security Center Windows y Kaspersky Security Center Linux, realice una de las siguientes acciones:

   - Para la migración de MySQL o MariaDB a MySQL o MariaDB: cree una copia de seguridad con la utilidad klbackup o una tarea de copia de seguridad de datos en el dispositivo con el Servidor de administración instalado.
   - Para la migración de PostgreSQL a PostgreSQL y de Postgres Pro a Postgres Pro: cree una copia de seguridad mediante la utilidad klbackup o una tarea de copia de seguridad de datos en el dispositivo con el Servidor de administración instalado.
   - Para la migración de Microsoft SQL Server a MySQL o MariaDB: cree una copia de seguridad con la utilidad klbackup, con la opción **Migrar al formato de MySQL/MariaDB** habilitada.
   - Para la migración de Microsoft SQL Server a PostgreSQL o Postgres Pro:

     1. Para admitir la migración a PostgreSQL y Postgres Pro, envíe una solicitud al Soporte técnico de Kaspersky e instale el parche 15.1.0.20748-pf2 para el Servidor de administración.

        O bien, puede actualizar Kaspersky Security Center Windows a la versión 15.1.0.22239.

     2. Cree una copia de seguridad con la utilidad klbackup.

        Si ejecuta klbackup desde la línea de comandos, use el indicador `-migrate postgres`.

        Si usa la interfaz de klbackup, habilite la opción **Migrar al formato de Postgres**.

   Después de crear una copia de seguridad, desconecte el Servidor de administración de Kaspersky Security Center Windows de la red.

3. **Preparación de un nuevo dispositivo para la instalación de Kaspersky Security Center Linux**

   En esta etapa del escenario, puede hacer lo siguiente:

   1. Seleccione un nuevo dispositivo para instalar el Servidor de administración. Este dispositivo debe cumplir con los requisitos de hardware y software. Compruebe que los puertos utilizados en el Servidor de administración estén disponibles.
   2. Asigne la misma dirección al nuevo dispositivo.

      Al nuevo Servidor de Administración se le puede asignar un nombre NetBIOS, un FQDN y una dirección IP estática. Esto depende de la dirección del Servidor de administración que se haya configurado en el paquete de instalación del Agente de red cuando se desplegaron los agentes de red. Como alternativa, puede usar la dirección de conexión que determina el Servidor de administración al que se conecta el Agente de red (puede obtener esta dirección en los dispositivos administrados mediante la utilidad klnagchk).

4. **Instalación y configuración del DBMS**

   En esta etapa del escenario, puede hacer lo siguiente:

   1. Seleccione el tipo de DBMS que mejor rendimiento ofrezca. Tenga en cuenta la cantidad de dispositivos conectados a la red, la topología y la carga de trabajo de la red. Puede elegir uno de los DBMS compatibles.
   2. Instale el DBMS que corresponda al tipo de DBMS que seleccionó al crear la copia de seguridad. Para obtener información sobre cómo instalar el DBMS seleccionado, consulte su documentación.

La nueva versión de la base de datos no debe ser inferior a la vigente.

3. Configure el DBMS para trabajar con Kaspersky Security Center Linux.

**5 Instalación de Kaspersky Security Center Linux**

Instale Kaspersky Security Center Linux en el nuevo dispositivo.

La cuenta de usuario interna del administrador creada durante la instalación, así como otros objetos (grupos, directivas, tareas, usuarios) creados antes de restaurar los datos del Servidor de administración desde la copia de seguridad, se perderán después de la restauración. Estos objetos serán reemplazados por objetos contenidos en la copia de seguridad.

**6 Restauración de los datos del Servidor de administración a partir de la copia de seguridad**

En esta etapa del escenario, puede hacer lo siguiente:

1. Restaurar los datos del Servidor de administración en el nuevo dispositivo mediante la utilidad klbackup.

2. Si no tenía la cuenta de usuario interna del administrador con la que inició sesión en el Servidor de administración Kaspersky Security Center Windows y utilizó una cuenta local de Windows o una cuenta de dominio, cree una cuenta de administrador utilizando la utilidad kladduser de la siguiente manera:

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>
   ```

   donde el parámetro `<password>` cumple los siguientes requisitos:

   - La contraseña de usuario no puede tener menos de 8 caracteres ni más de 256.
   - La contraseña debe incluir caracteres de al menos tres de los grupos enumerados a continuación:
     - Letras mayúsculas (A-Z)
     - Letras minúsculas (a-z)
     - Números (0-9)
     - Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

**7 Instalar Kaspersky Security Center Web Console y configurar el Servidor de administración**

En esta etapa del escenario, puede hacer lo siguiente:

1. Instalación de Kaspersky Security Center Web Console.

   Si Kaspersky Security Center Web Console se ha instalado anteriormente, vuelva a instalarlo con el mismo archivo de respuesta.

   Iniciar sesión en Kaspersky Security Center Web Console con la cuenta de usuario interna del administrador.

   Después de restaurar los datos del Servidor de administración, el proceso de inicialización puede durar hasta 15 minutos, aunque el tiempo exacto dependerá del rendimiento del hardware y del tamaño de los datos. Durante este tiempo, es posible que Kaspersky Security Center Web Console no se conecte y muestre errores.

2. Una vez que la inicialización de los datos en la base de datos haya finalizado, asegúrese de comprobar que las principales funciones del Servidor de administración funcionen como es debido. Verifique que el Servidor de administración se sincronice con los dispositivos administrados y que se hayan restaurado los datos del Servidor de administración.

3. Sondee los controladores de dominio, para recuperar información sobre la estructura del dominio, las cuentas de usuario, los grupos de seguridad y los nombres DNS de los dispositivos incluidos en el dominio.

4. Si es necesario, desinstale el Servidor de administración y el servidor de bases de datos del dispositivo antiguo.

   No debe haber varios servidores de administración en la misma red con la misma dirección de conexión y certificado de Servidor de administración.

El administrador tendrá acceso a los mismos datos del Servidor de administración y a los mismos dispositivos administrados que estaban disponibles en Kaspersky Security Center Windows, teniendo en cuenta la disponibilidad de funciones de Kaspersky Security Center Linux.

# Migración a Kaspersky Security Center Linux a través del Asistente de migración

En este escenario, puede transferir la estructura del grupo de administración, incluidos los dispositivos administrados y otros objetos de grupo (directivas, tareas, tareas globales, etiquetas y selecciones de dispositivos) desde Kaspersky Security Center Windows bajo la administración de Kaspersky Security Center Linux. Antes de la migración, asegúrese de que las funciones de Kaspersky Security Center Windows que necesite estén disponibles en Kaspersky Security Center Linux.

Limitaciones:

- La migración solo es posible desde Kaspersky Security Center Windows (versión 14.2 o posterior) a Kaspersky Security Center Linux (versión 15 o posterior).
- Solo puede realizar este escenario mediante el uso de Kaspersky Security Center Web Console.

## Etapas

El escenario de migración se desarrolla en etapas:

1. **Elija un método de migración**

   Debe realizar la migración a Kaspersky Security Center Linux a través del Asistente de migración. Los pasos del Asistente de migración dependen de si los Servidores de administración de Kaspersky Security Center Windows y Kaspersky Security Center Linux están organizados en una jerarquía:

   - Migración con una jerarquía de Servidores de administración

     Elija esta opción si el Servidor de administración de Kaspersky Security Center Windows actúa como Servidor secundario del Servidor de administración de Kaspersky Security Center Linux. Usted podrá encargarse del proceso de migración y cambiar de un Servidor a otro utilizando una sola instancia de Kaspersky Security Center Web Console. Si prefiere esta opción, puede organizar los Servidores de administración en una jerarquía para simplificar el procedimiento de migración. Para hacerlo, cree la jerarquía antes de iniciar la migración.

   - Migración con un archivo de exportación (archivo ZIP)

     Elija esta opción si los Servidores de administración de Kaspersky Security Center Windows y Kaspersky Security Center Linux no están organizados en una jerarquía. Para llevar a cabo la migración, puede utilizar dos instancias de Kaspersky Security Center Web Console: una para Kaspersky Security Center Windows y otra para Kaspersky Security Center Linux. En este caso, utilizará el archivo de exportación que creó y descargó durante la exportación desde Kaspersky Security Center Windows e importará este archivo a Kaspersky Security Center Linux.

2. **Cree una copia de seguridad del certificado y la clave privada del Servidor de administración de Kaspersky Security Center Windows (paso opcional)**

   Es posible que desee poner los dispositivos administrados bajo la administración del Servidor de administración de Kaspersky Security Center Linux mediante la restauración del certificado y la clave privada del Servidor de administración a partir de una copia de seguridad. En este caso, haga una copia de seguridad del certificado y la clave privada del Servidor de administración de Kaspersky Security Center Windows. Luego, en la etapa 6, restaure el certificado y la clave privada.

3. **Exportación de datos desde Kaspersky Security Center Windows**

   Abra Kaspersky Security Center Windows y, luego, ejecute el Asistente de migración.

4. **Importe datos a Kaspersky Security Center Linux**

   Continúe con el Asistente de migración para importar los datos exportados a Kaspersky Security Center Linux. Si los servidores están organizados en una jerarquía, la importación se inicia de forma automática después de una exportación exitosa dentro del mismo asistente. Si los servidores no están organizados en una jerarquía, continúe con el Asistente de migración después de cambiar a Kaspersky Security Center Linux.

5. **Realice acciones adicionales para transferir objetos y configuraciones de Kaspersky Security Center Windows a Kaspersky Security Center Linux de forma manual (paso opcional)**

   También es posible transferir los objetos y las configuraciones que no se pueden transferir a través del Asistente de migración. Por ejemplo, también puede hacer lo siguiente:

   - Transferir las claves de licencia que utilizó el Servidor de administración y las aplicaciones administradas
   - Configurar tareas globales del Servidor de administración
   - Configurar los ajustes de la directiva del Agente de red
   - Crear paquetes de instalación de aplicaciones
   - Crear Servidores virtuales
   - Asignar y configurar puntos de distribución
   - Configurar reglas de movimiento de dispositivos
   - Configurar reglas para etiquetar dispositivos de forma automática
   - Crear categorías de aplicaciones

6. **Mueva los dispositivos administrados importados bajo la administración de Kaspersky Security Center Linux:**

   Para completar la migración, mueva los dispositivos administrados importados bajo la administración de Kaspersky Security Center Linux. Puede hacerlo usando uno de los siguientes métodos:

   - Mediante la utilidad klmover

     Use la utilidad klmover y especifique la configuración de conexión para el nuevo Servidor de administración.

   - Mediante la tarea *Cambiar Servidor de administración*

     Cree una tarea *Cambiar Servidor de administración*, especifique los dispositivos administrados importados, el nuevo Servidor de administración y otras configuraciones de la tarea. Luego, ejecute la tarea para poner los dispositivos administrados bajo la administración del Servidor de administración de Kaspersky Security Center Linux.

- Mediante la eliminación (si ya está instalado) y la instalación posterior del Agente de red en los dispositivos administrados

  Cree un nuevo paquete de instalación del Agente de red y especifique la configuración de conexión para el nuevo Servidor de administración en las propiedades del paquete de instalación. Elimine el Agente de red en los dispositivos administrados importados y, luego, use el paquete de instalación para instalar el Agente de red en los dispositivos administrados importados a través de una tarea de instalación remota. También puede crear y utilizar un paquete de instalación independiente para instalar el Agente de red de manera local. Para obtener más información, consulte Cambio de dispositivos administrados bajo la administración de Kaspersky Security Center Linux.

- Restaurando el certificado y la clave privada del Servidor de administración desde una copia de seguridad (solo para la migración a Kaspersky Security Center Linux 15.1 o posterior).

  Asigne al dispositivo que aloja el Servidor de administración de Kaspersky Security Center Linux la misma dirección IP asignada al Servidor de administración de Kaspersky Security Center Windows. Ejecute la utilidad klbackup con el parámetro `-cert_only` para restaurar el certificado del Servidor de administración y la clave privada desde la copia de seguridad que ha guardado en la etapa 2. En la línea de comandos, ejecute el siguiente comando: `/opt/kaspersky/ksc64/sbin/klbackup -path < ruta a la copia de seguridad del certificado del Servidor de administración > -restore -cert_only` . Para obtener más información, consulte Uso de la utilidad klbackup para mover los dispositivos administrados y ponerlos bajo la administración de otro Servidor de administración.

7. **Actualice el Agente de red a la versión más reciente**

   Le recomendamos que actualice el Agente de red para Linux a la misma versión que Kaspersky Security Center.

8. **Asegúrese de que los dispositivos administrados estén visibles en el nuevo Servidor de administración**

   En el Servidor de administración de Kaspersky Security Center Linux, abra la lista de dispositivos administrados (**Activos (dispositivos)** → **Dispositivos administrados**) y verifique los valores en las columnas **Visible**, **Agente de red instalado** y **Última conexión con el Servidor de administración**.

## Otros métodos de migración de datos

Además del asistente de migración, también puede transferir tareas y directivas específicas:

- Exporte las tareas de Kaspersky Security Center Windows y, luego, impórtelas en Kaspersky Security Center Linux.
- Exporte directivas específicas de Kaspersky Security Center Windows y luego impórtelas en Kaspersky Security Center Linux. Los perfiles de las directivas que seleccione se exportarán e importarán junto con las directivas.

## Exportación de objetos de grupo desde Kaspersky Security Center Windows

La estructura del grupo de administración de la migración, incluidos los dispositivos administrados y otros objetos de grupo de Kaspersky Security Center Windows a Kaspersky Security Center Linux, requiere que primero seleccione los datos para exportar y cree un archivo de exportación. El archivo de exportación contiene información sobre todos los objetos de grupo que desea migrar. El archivo de exportación se utilizará para la importación posterior a Kaspersky Security Center Linux.

Puede exportar los siguientes objetos:

- Tareas y directivas de aplicaciones administradas
- Tareas globales

- Selecciones de dispositivos personalizados
- Estructura del grupo de administración y dispositivos incluidos
- Etiquetas que se asignaron a los dispositivos en migración

Antes de iniciar la exportación, lea la información general sobre la migración a Kaspersky Security Center Linux. Elija el método de migración: puede utilizar o no la jerarquía de servidores de administración de Kaspersky Security Center Windows y Kaspersky Security Center Linux.

*Para exportar dispositivos administrados y objetos afines a través del Asistente de migración, haga lo siguiente:*

1. Realice una de las siguientes acciones (dependiendo de si los servidores de administración de Kaspersky Security Center Windows y Kaspersky Security Center Linux están organizados en una jerarquía):
   - Si los servidores están organizados en una jerarquía, abra Kaspersky Security Center Web Console y cambie al servidor de Kaspersky Security Center Windows.
   - Si los servidores no están organizados en una jerarquía, abra una instancia de Kaspersky Security Center Web Console conectada a Kaspersky Security Center Windows.
2. En el menú principal, vaya a **Operaciones** → **Migración**.
3. Para iniciar el asistente y seguir los pasos, seleccione a dónde desea transferir sus datos y la configuración.
   - Si desea transferir sus datos y la configuración a Kaspersky Security Center Cloud Console, seleccione **Migrar a Kaspersky Security Center Cloud Console**.
   - Si desea transferir sus datos y configuración a Kaspersky Security Center Linux o Kaspersky Next XDR Expert, seleccione **Migrar a Kaspersky Security Center Linux o a Open Single Management Platform**.
4. Seleccione el grupo o subgrupo de administración que desee exportar. Asegúrese de que el grupo o subgrupo de administración seleccionado no tenga más de 10 000 dispositivos.
5. Seleccione las aplicaciones administradas cuyas tareas y directivas desee exportar. Seleccione solo aquellas aplicaciones que sean compatibles con Kaspersky Security Center Linux. Los objetos de las aplicaciones incompatibles se exportarán de todos modos, pero no podrán utilizarse.
6. Utilice los vínculos que verá en el lado izquierdo para seleccionar las tareas globales, las selecciones de dispositivos y los informes que desee exportar. Puede usar el vínculo **Objetos de grupo** para excluir los roles personalizados, los usuarios internos, los grupos de seguridad internos y las categorías de aplicaciones personalizadas que no desee exportar.

Se crea el archivo de exportación (archivo ZIP). Dependiendo de si realiza o no una migración compatible con la jerarquía del Servidor de administración, el archivo de exportación se guarda de la siguiente manera:

- Si los Servidores están organizados en una jerarquía, el archivo de exportación se guarda en la carpeta temporal del servidor de Kaspersky Security Center Web Console.
- Si los Servidores no están organizados en una jerarquía, el archivo de exportación se descarga en su dispositivo.

Para una migración compatible con la jerarquía del Servidor de administración, la importación se inicia automáticamente después de una exportación exitosa. Para una migración no compatible con la jerarquía del Servidor de administración, puede importar manualmente el archivo de exportación guardado a Kaspersky Security Center Linux.

## Importar el archivo de exportación en Kaspersky Security Center Linux

Para transferir información sobre dispositivos administrados, objetos y sus configuraciones que exportó desde Kaspersky Security Center Windows, debe importarla a Kaspersky Security Center Linux o Kaspersky Next XDR Expert.

*Para importar dispositivos administrados y objetos afines a través del Asistente de migración, haga lo siguiente:*

1. Realice una de las siguientes acciones (dependiendo de si los servidores de administración de Kaspersky Security Center Windows y Kaspersky Security Center Linux están organizados en una jerarquía):

   - Si los servidores están organizados en una jerarquía, continúe con el siguiente paso del Asistente de migración una vez completada la exportación. La importación comienza automáticamente después de una exportación exitosa dentro de este asistente (consulte el paso 2 de esta instrucción).

   - Si los Servidores no están organizados en una jerarquía:

     a. Abra Kaspersky Security Center Web Console conectada a Kaspersky Security Center Linux o Kaspersky Next XDR Expert.

     b. En el menú principal, vaya a **Operaciones** → **Migración**.

     c. Seleccione el archivo de exportación (archivo ZIP) que creó y descargó durante la exportación desde Kaspersky Security Center Windows. Se iniciará la carga del archivo de exportación.

2. Una vez que el archivo de exportación se haya cargado correctamente, podrá continuar con la importación. Si desea especificar otro archivo de exportación, haga clic en el vínculo **Cambiar** y, luego, seleccione el archivo deseado.

3. Se muestra toda la jerarquía de grupos de administración de Kaspersky Security Center Linux.

   Seleccione la casilla de verificación junto al grupo de administración de destino al que se deben restaurar los objetos de grupo de administración exportado (dispositivos administrados, directivas, tareas y otros objetos de grupo).

4. Comenzará la importación de objetos de grupo. No podrá minimizar el Asistente de migración ni realizar ninguna operación simultánea durante la importación. Espere a que los íconos de actualización (🔄) ubicados junto a los elementos de la lista de objetos cambien por marcas de verificación verdes (✓) y se complete la importación.

5. Una vez que concluya la importación, verá la estructura de grupos de administración exportada (incluidos los detalles de los dispositivos) en el grupo de administración de destino que haya seleccionado. Si intenta restaurar un objeto que tenga el mismo nombre que un objeto existente, se agregará un sufijo secuencial al nombre del objeto restaurado.

Si una tarea migrada contiene los datos de la cuenta con la cual ha de ejecutarse, una vez que se complete la importación, deberá abrir la tarea e ingresar la contraseña nuevamente.

Si la importación se completó con un error, puede realizar una de las siguientes acciones:

- Para la migración con soporte de jerarquía del Servidor de administración, puede comenzar a importar el archivo de exportación nuevamente.
- Para la migración sin compatibilidad con la jerarquía del Servidor de administración, puede iniciar el Asistente de migración para seleccionar otro archivo de exportación y luego importarlo nuevamente.

Puede comprobar si los objetos de grupo incluidos en el alcance de la exportación se han importado correctamente a Kaspersky Security Center Linux. Para ello, vaya a la sección **Activos (dispositivos)** y asegúrese de que los objetos importados aparezcan en las subsecciones correspondientes.

Tenga en cuenta que los dispositivos administrados importados se muestran en la subsección **Dispositivos administrados**, pero son invisibles en la red y el Agente de red si no estás instalados ni ejecutándose en ellos (el valor *No* en las columnas **Visible**, **Agente de red instalado** y **Agente de red en ejecución**

Para completar la migración, debe cambiar los dispositivos administrados para que estén bajo la administración de Kaspersky Security Center Linux.

## Cambiar los dispositivos administrados para que estén bajo la administración de Kaspersky Security Center Linux

Después de una importación exitosa de información sobre dispositivos administrados, objetos y su configuración a Kaspersky Security Center Linux, debe cambiar los dispositivos administrados para que estén bajo la administración de Kaspersky Security Center Linux para completar la migración.

Puede mover los dispositivos administrados para que estén bajo Kaspersky Security Center Linux mediante uno de los siguientes métodos:

- Con la utilidad klmover.
- Usar la tarea *Cambiar Servidor de administración*.
- Restaurar el certificado y la clave privada del Servidor de administración a partir de una copia de seguridad (solo para la migración a Kaspersky Security Center Linux 15.1 o posterior).

  Para obtener más información, consulte la etapa 6 del escenario de migración principal.
- Mediante la instalación del Agente de red en los dispositivos administrados a través de una tarea de instalación remota.

*Para cambiar los dispositivos administrados para que estén bajo la administración de Kaspersky Security Center Linux instalando el Agente de red:*

1. Elimine el Agente de red en los dispositivos administrados importados que se cambiarán bajo la administración de Kaspersky Security Center Linux.
2. Cambie al Servidor de Administración de Kaspersky Security Center Windows.
3. Vaya a **Descubrimiento y despliegue** → **Despliegue y asignación** → **Paquetes de instalación** y luego abra las propiedades de un paquete de instalación existente del Agente de red.

   Si el paquete de instalación del Agente de red no está en la lista de paquetes, descargue uno nuevo.

   También puede crear y utilizar un paquete de instalación independiente para instalar el Agente de red de manera local.

4. En la pestaña **Configuración**, seleccione la sección **Conexión**. Defina los ajustes de conexión del Servidor de administración de Kaspersky Security Center Linux.

5. Cree una tarea de instalación remota para dispositivos administrados importados y, luego, especifique el paquete de instalación del Agente de red reconfigurado.

   Puede instalar el Agente de red a través del Servidor de administración de Kaspersky Security Center Windows o mediante un dispositivo basado en Windows que actúa como punto de distribución. Si utiliza el Servidor de administración, habilite la opción **Con los recursos del sistema operativo a través del Servidor de administración**. Si utiliza un punto de distribución, habilite la opción **Con los recursos del sistema operativo a través de los puntos de distribución**.

6. Ejecute la tarea de instalación remota.

Una vez que la tarea de instalación remota finalice exitosamente, vaya al Servidor de administración de Kaspersky Security Center Linux y asegúrese de que los dispositivos administrados estén visibles en la red y que el Agente de red esté instalado y ejecutándose en ellos (el valor *Sí* en **Visible**, **Agente de red instalado** y **Agente de red en ejecución** columnas).

# Iniciar y cerrar sesión en Kaspersky Security Center Web Console

Una vez que instale el Servidor de administración y el Servidor de Web Console, podrá iniciar sesión en Kaspersky Security Center Web Console. Debe conocer la dirección web del Servidor de administración y el número de puerto especificado durante la instalación (de forma predeterminada, el puerto es 8080). En su navegador, JavaScript debe estar habilitado.

Para iniciar sesión en Kaspersky Security Center Web Console, utilice los siguientes métodos:

- Mediante el uso de autenticación de dominio

  > Si elige este método, asegúrese de que Sondeo del control de dominio se haya activado y de que los usuarios del dominio se hayan agregado al Servidor de administración.

- Ingresar el nombre de usuario y la contraseña del dominio
- Ingresar el nombre de usuario y la contraseña del administrador

## Iniciar sesión mediante la autenticación de dominio

*Para iniciar sesión en Kaspersky Security Center Web Console con la autenticación de dominio:*

1. En su navegador, vaya a https://`<dirección de Kaspersky Security Center Web Console>`:`<Número de puerto>`

   Se muestra la página de inicio de sesión.

2. Si agregó varios servidores de confianza, en la lista Servidores de administración, seleccione el Servidor de administración al que desea conectarse.

   Si solo agregó un único Servidor de administración, no verá una lista de servidores de administración.

3. Realice una de las siguientes acciones:

   - Haga clic en el botón **Utilizar autenticación de dominio**.
   - Si el Servidor tiene uno o más Servidores de administración virtuales y desea iniciar sesión en uno de ellos usando la autenticación de dominio:

     a. Haga clic en **Mostrar opciones de Servidor virtual**.

     b. Escriba el nombre del Servidor de administración virtual que especificó cuando creó el servidor virtual.

     c. Haga clic en el botón **Utilizar autenticación de dominio**.

4. Si la verificación en dos pasos está habilitada en su cuenta, especifique el código de seguridad que generó la app de autenticación en el dispositivo móvil.

   Si es necesario, puede regresar a la página de inicio de sesión.

Una vez que inicie sesión, verá el panel en el idioma y con el tema que haya utilizado en el inicio de sesión anterior. Puede navegar por Kaspersky Security Center Web Console y usarlo para trabajar con Kaspersky Security Center.

## Iniciar sesión especificando el nombre de usuario y la contraseña del administrador

*Para iniciar sesión en Kaspersky Security Center Web Console especificando el nombre de usuario y la contraseña del administrador:*

1. En su navegador, vaya a https://`<dirección de Kaspersky Security Center Web Console>`:`<Número de puerto>`

   Se muestra la página de inicio de sesión.

2. Si agregó varios servidores de confianza, en la lista Servidores de administración, seleccione el Servidor de administración al que desea conectarse.

   Si solo agregó un único Servidor de administración, no verá una lista de servidores de administración.

3. Realice una de las siguientes acciones:

- Para iniciar sesión en el Servidor de administración con una cuenta de usuario de dominio:

  a. Ingrese el nombre de usuario y la contraseña del usuario del dominio.

  Puede ingresar el nombre del usuario del dominio en uno de los siguientes formatos:

  - `Nombre de usuario@dns.domain`
  - `NTDOMAIN\Nombre de usuario`

  b. Haga clic en el botón **Entrar**.

  Antes de iniciar sesión con una cuenta de usuario de dominio, sondee el controlador de dominio para obtener la lista de usuarios del dominio.

- Para iniciar sesión en el Servidor de administración:

  a. Ingrese el nombre de usuario y la contraseña del administrador local.

  b. Haga clic en el botón **Entrar**.

- Si el Servidor tiene uno o más servidores de administración virtuales y desea iniciar sesión en uno de ellos, haga lo siguiente:

  a. Haga clic en **Mostrar opciones de Servidor virtual**.

  b. Escriba el nombre del Servidor de administración virtual que especificó cuando creó el servidor virtual.

  c. Ingrese el nombre de usuario y la contraseña del administrador que tiene derechos en el Servidor de administración virtual.

  d. Haga clic en el botón **Entrar**.

4. Si la verificación en dos pasos está habilitada en su cuenta, especifique el código de seguridad que generó la app de autenticación en el dispositivo móvil.

   Si es necesario, puede regresar a la página de inicio de sesión.

5. Si el cambio de contraseña forzado está habilitado en su cuenta o su contraseña ha caducado, aparecerá la ventana de cambio de contraseña. Establezca una nueva contraseña para iniciar sesión en Kaspersky Security Center Web Console.

Una vez que inicie sesión, verá el panel en el idioma y con el tema que haya utilizado en el inicio de sesión anterior. Puede navegar por Kaspersky Security Center Web Console y usarlo para trabajar con Kaspersky Security Center.

## Cierre de sesión

*Para cerrar sesión en Kaspersky Security Center Web Console,*

En el menú principal, vaya a los ajustes de su cuenta y haga clic en **Salir**.

Kaspersky Security Center Web Console se cierra y se muestra la página de inicio de sesión.

# Identity and Access Manager en Kaspersky Security Center Web Console

Esta sección proporciona información sobre Identity and Access Manager (también conocido como IAM).

## Acerca de Identity and Access Manager

*Identity and Access Manager* (también conocido como IAM) es un componente de la Kaspersky Security Center Web Console que le permite utilizar un inicio de sesión único (SSO) entre Kaspersky Security Center Web Console y la interfaz web de Kaspersky Industrial CyberSecurity for Networks. IAM utiliza el protocolo OAuth 2.0 para garantizar la autorización de Kaspersky Industrial CyberSecurity for Networks en Kaspersky Security Center Web Console.

En este caso, Kaspersky Industrial CyberSecurity for Networks, a la que puede acceder a través de Kaspersky Security Center Web Console, se conoce como un *servidor de recursos*, y Kaspersky Security Center Web Console y la interfaz web de Kaspersky Industrial CyberSecurity for Networks se denominan *clientes de OAuth 2.0*. Un servidor de recursos es un programa que funciona con varios usuarios y requiere autorización. El cliente usa un *token* para la autorización en el servidor de recursos. Un token es una secuencia única de bytes. Cuando un token caduca, se vuelve a emitir automáticamente. IAM actúa como un servidor único de autorización para varios clientes OAuth 2.0.

Puede instalar IAM al instalar Kaspersky Security Center Web Console. Puede habilitarlo más tarde en cualquier momento en la configuración de Kaspersky Security Center Web Console. Si un servidor de Kaspersky Industrial CyberSecurity o una interfaz web de Kaspersky Industrial CyberSecurity están instalados en un dispositivo administrado por el mismo Servidor de administración, IAM detecta este programa y se muestra una notificación en Kaspersky Security Center Web Console con información al respecto. Puede registrar Kaspersky Industrial CyberSecurity for Networks y luego usar SSO para Kaspersky Security Center Web Console y una interfaz web de Kaspersky Industrial CyberSecurity for Networks.

Si cierra sesión en Kaspersky Security Center Web Console, su sesión en la interfaz web de Kaspersky Industrial CyberSecurity for Networks finalizará y tendrá que iniciar sesión en Kaspersky Security Center Web Console nuevamente.

## Habilitación de Identity and Access Manager: escenario

### Requisitos previos

Antes de comenzar, asegúrese de tener acceso a Kaspersky Industrial CyberSecurity for Networks versión 3.1 o posterior.

### Etapas

La habilitación de Identity and Access Manager (también denominada IAM) se realiza en etapas:

1. **Comprobar los puertos necesarios**

   Asegúrese de que los puertos 3333, 4004 y 4444 estén abiertos en el dispositivo donde está instalado Kaspersky Security Center Web Console. Estos puertos son necesarios para usar OAuth 2.0. Si lo desea, puede cambiar los números de puerto predeterminados en la ventana de configuración de Kaspersky Security Center Web Console.

   Además de los puertos 3333, 4004 y 4444, Kaspersky Security Center Web Console también usa los puertos 4445, 2444 y 2445 para diferentes propósitos.

2. **Instalación de Identity and Access Manager**

   Durante la instalación de Kaspersky Security Center Web Console, especifique que desea instalar Identity and Access Manager. Si no lo hizo, vuelva a ejecutar el Asistente de instalación de Kaspersky Security Center Web Console.

3. **Configuración de Identity and Access Manager**

   En la ventana de configuración de Kaspersky Security Center Web Console, asegúrese de que el botón de alternancia **Identity and Access Manager (IAM)** esté habilitado. Además, especifique el nombre DNS del dispositivo donde está instalado Kaspersky Security Center Web Console: las aplicaciones cliente se conectarán a este dispositivo.

4. **Especificar la configuración del token**

   En la ventana de configuración de Kaspersky Security Center Web Console, especifique la duración de los tokens y el tiempo de espera de autorización que utilizará Identity and Access Manager. Puede utilizar los valores predeterminados o puede especificar sus propios valores de acuerdo con sus necesidades.

5. **Concesión de certificados**

   Si prefiere utilizar los certificados generados por el Servidor de administración, en la ventana de configuración de Kaspersky Security Center Web Console, descargue los certificados de origen para los puertos utilizados por IAM y distribúyalos en las estaciones de trabajo de los usuarios de Kaspersky Security Center Web Console. De lo contrario, los navegadores de los usuarios mostrarán mensajes de error cuando intenten conectarse a Kaspersky Security Center Web Console.

6. **Registro de servidores de Kaspersky Industrial CyberSecurity for Networks e interfaces web de Kaspersky Industrial CyberSecurity for Networks**

   Cuando se instala IAM, Kaspersky Security Center Web Console muestra un mensaje que indica que un servidor (o varios servidores) de Industrial CyberSecurity for Networks y una o varias interfaces web de Kaspersky Industrial CyberSecurity for Networks están esperando ser registrados. Haga clic en este mensaje para registrar su servidor (o varios servidores) e interfaz web (o varias interfaces web) de Kaspersky Industrial CyberSecurity for Networks.

## Resultados

Después de completar este escenario, podrá usar SSO e IAM para Kaspersky Industrial CyberSecurity for Networks y Kaspersky Security Center Web Console.

# Configuración de Identity and Access Manager en Kaspersky Security Center Web Console

*Para configurar Identity and Access Manager según sus necesidades, haga lo siguiente:*

1. En el menú principal, vaya a **Configuración** → **Identity and Access Manager**.
2. En la sección **Identity and Access Manager**, asegúrese de que Identity and Access Manager esté habilitado.
3. Haga clic en el vínculo **Configuración** en la línea **Nombre de la red del dispositivo con Identity and Access Manager**.
4. Especifique el nombre DNS del dispositivo en el que instaló Identity and Access Manager. Las aplicaciones cliente se conectarán a este dispositivo.
5. Si lo desea, cambie la configuración de token predeterminada, la configuración de certificado y los números de puerto haciendo clic en el enlace **Configuración** debajo del grupo relevante de ajustes.

Identity and Access Manager está habilitado y funciona de acuerdo con sus necesidades.

# Registro de la aplicación Kaspersky Industrial CyberSecurity for Networks en Kaspersky Security Center Web Console

Para comenzar a trabajar con la aplicación de Kaspersky Industrial CyberSecurity for Networks a través de Kaspersky Security Center Web Console, primero debe registrarlo en Kaspersky Security Center Web Console.

Para registrar la aplicación de Kaspersky Industrial CyberSecurity for Networks:

1. Asegúrese de que se cumplan estos requisitos:

   - Descargó e instaló el complemento web de Kaspersky Industrial CyberSecurity for Networks.

     (Puede ocuparse de esto más adelante, mientras el servidor de Kaspersky Industrial CyberSecurity for Networks se sincroniza con el Servidor de administración).

   - Haber completado el Escenario de preparativos para el uso de la tecnología de inicio de sesión único (SSO).

   - La configuración necesaria en la interfaz web de Kaspersky Industrial CyberSecurity for Networks se especifica en la página de Kaspersky Security Center. Para obtener más información, consulte la Ayuda en línea de Kaspersky Industrial CyberSecurity for Networks.

   - Haber iniciado sesión en Kaspersky Security Center Web Console con una cuenta de administrador.

   - Que IAM esté configurado.

2. Mueva el dispositivo donde está instalado Kaspersky Industrial CyberSecurity for Networks Server del grupo Dispositivos no asignados al grupo Dispositivos administrados:

   a. En el menú principal, vaya a **Descubrimiento y despliegue** → **Dispositivos no asignados**.

   b. Seleccione la casilla de verificación ubicada junto al dispositivo donde está instalado Kaspersky Industrial CyberSecurity for Networks Server.

   c. Haga clic en el botón **Mover a un grupo**.

   d. En la jerarquía de grupos de administración, seleccione la casilla de verificación ubicada junto al grupo Dispositivos administrados.

   e. Haga clic en el botón **Mover**.

3. Vaya a las propiedades del dispositivo donde está instalado Kaspersky Industrial CyberSecurity for Networks Server.

4. En la página de propiedades del dispositivo, en la sección **General**, seleccione la opción **No desconectarse del Servidor de Administración** y, a continuación, haga clic en el botón **Guardar**.

5. En la página de propiedades del dispositivo, seleccione la sección **Aplicaciones**.

6. En la sección **Aplicaciones**, seleccione el Agente de red de Kaspersky.

7. Si el estado actual de la solicitud es *Detenido*, espere hasta que cambie a *En ejecución*.

   Esto puede tardar hasta 15 minutos. Si aún no ha instalado el complemento web de Kaspersky Industrial CyberSecurity for Networks, puede hacerlo ahora, mientras espera.

8. En el menú principal, vaya a **Configuración** → **Identity and Access Manager**.

   En el campo **Solicitudes de registro**, se muestra una solicitud pendiente.

9. Haga clic en el enlace **Ajustes** ubicado debajo del campo **Solicitudes de registro**.

10. En la lista de clientes registrados que se abre, seleccione la casilla de verificación ubicada junto al nombre del Kaspersky Industrial CyberSecurity for Networks Server que tiene el estado *Pendiente* y, a continuación, haga clic en el botón **Aprobar**.

    Si no desea registrar Kaspersky Industrial CyberSecurity for Networks Server, puede hacer clic en el botón Rechazar y volver a esta lista más tarde.

    Después de hacer clic en el botón **Aprobar**, el estado cambia a *Aprobado* y luego a *Listo*. Si el estado no cambia, puede hacer clic en el botón Actualizar.

11. Cierre la lista de clientes registrados y asegúrese de que el valor en el campo **Clientes registrados** haya aumentado.

12. Para agregar el widget de Kaspersky Industrial CyberSecurity for Networks en el panel:

    a. En el menú principal, vaya a **Supervisión e informes** → **Panel**.

    b. En el panel, haga clic en el botón **Agregar o restaurar widget web**.

    c. En el menú del widget que se abre, seleccione **Otros**.

    d. Seleccione el widget Kaspersky Industrial CyberSecurity for Networks.

    Ahora puede pasar a la interfaz web de Kaspersky Industrial CyberSecurity for Networks mediante el enlace del widget.

Después de completar el procedimiento de registro, aparecerá un nuevo botón, **Kaspersky Security Center**, en la página de inicio de sesión de la interfaz web de Kaspersky Industrial CyberSecurity for Networks. Puede hacer clic en este botón para iniciar sesión en la interfaz web de Kaspersky Industrial CyberSecurity for Networks con sus credenciales de Kaspersky Security Center.

# Duración de los tokens y tiempo de espera de autorización para Identity and Access Manager

Al configurar Identity and Access Manager (también conocido como IAM), debe especificar la configuración para la duración del token y el tiempo de espera de autorización. La configuración predeterminada está diseñada para reflejar tanto los estándares de seguridad como la carga del servidor. Sin embargo, puede cambiar esta configuración de acuerdo con las directivas de su organización.

IAM vuelve a emitir automáticamente un token cuando está a punto de caducar.

La siguiente tabla enumera la configuración predeterminada de la duración del token.

Configuración de la duración del token

| Token | Duración predeterminada (en segundos) | Descripción |
|---|---|---|
| **Token de identidad (id_token)** | 86400 | Token de identidad utilizado por el cliente OAuth 2.0 (es decir, Kaspersky Security Center Web Console o la consola de Kaspersky Industrial CyberSecurity). IAM envía el token de ID que contiene información sobre el usuario (es decir, el perfil de usuario) al cliente. |
| **Token de acceso (access_token)** | 86400 | Token de acceso utilizado por el cliente OAuth 2.0 para acceder al servidor de recursos en nombre del propietario del recurso identificado por IAM. |
| **Token de actualización (refresh_token)** | 172800 | El cliente OAuth 2.0 usa este token para volver a emitir el token de identidad y el token de acceso. |

La siguiente tabla enumera los tiempos de espera para auth_code y login_consent_request.

Configuración de tiempo de espera de autorización

| Configuración | Tiempo de espera predeterminado (en segundos) | Descripción |
|---|---|---|
| **Código de autorización (auth_code)** | 3600 | Tiempo de espera para intercambiar el código por el token. El cliente OAuth 2.0 envía este código al servidor de recursos y obtiene el token de acceso a cambio. |
| **Tiempo de espera de la solicitud de consentimiento de inicio de sesión (login_consent_request)** | 3600 | Tiempo de espera para delegar derechos de usuario al cliente de OAuth 2.0. |

Para obtener más información sobre los tokens, consulte el sitio web de OAuth.

*Para configurar el tiempo de espera para clientes cuya actividad del mouse o del teclado no se detecta:*

1. En la carpeta de instalación de Kaspersky Security Center Web Console, busque y abra el archivo config.json. El archivo contiene los parámetros para configurar el tiempo de espera para los clientes inactivos.

2. Use el parámetro `clientIdleTimeout` para especificar el tiempo (en milisegundos) después del cual un cliente inactivo mostrará una ventana emergente de advertencia.

3. Use el parámetro `clientLogoutTimeout` para especificar el tiempo (en milisegundos) después del cual finaliza la autorización de IAM para el cliente inactivo. El parámetro `clientLogoutTimeout` cuenta hacia atrás secuencialmente después del parámetro `clientIdleTimeout`.

# Descarga y distribución de certificados IAM

De forma predeterminada, Identity and Access Manager utiliza los certificados generados por el Servidor de administración para que los navegadores obtengan acceso a Kaspersky Security Center Web Console. Sin embargo, si lo desea, puede utilizar certificados personalizados. Independientemente del certificado que utilice, debe asegurarse de que todas las estaciones de trabajo desde las que los usuarios de Kaspersky Security Center Web Console acceden a Kaspersky Security Center Web Console confíen en este certificado.

*Para descargar y distribuir certificados, haga lo siguiente:*

1. En el menú principal, vaya a **Configuración → Identity and Access Manager**.
2. Para cada certificado, haga clic en el enlace **Configuración** debajo del grupo relevante de ajustes y luego realice una de las siguientes acciones:
   - Si desea utilizar el certificado que generó el Servidor de administración durante la instalación de Kaspersky Security Center Web Console, haga lo siguiente:
     1. Seleccione **Certificado generado por el Servidor de administración** en la ventana de propiedades del certificado que se abre.
     2. Haga clic en el botón **Descargar** para descargar el certificado.
     3. Distribuya el certificado descargado a todas las estaciones de trabajo desde las que los usuarios de Kaspersky Security Center Web Console acceden a Kaspersky Security Center Web Console.
   - Si tiene un certificado que desea utilizar, haga lo siguiente:
     1. Seleccione **Certificado TLS personalizado** en la ventana de propiedades del certificado que se abre.
     2. Seleccione el archivo de certificado y la clave privada.
     3. Haga clic en el botón **Aceptar**.
     4. Distribuya el certificado a todas las estaciones de trabajo desde las que los usuarios acceden a Kaspersky Security Center Web Console o la consola de Kaspersky Industrial CyberSecurity.

Los certificados otorgan a los usuarios acceso a Kaspersky Security Center Web Console y la consola de Kaspersky Industrial CyberSecurity.

Tiene que volver a emitir todos los certificados a tiempo. Los certificados generados por el Servidor de administración se deben volver a generar manualmente. Los certificados generados por el instalador de Kaspersky Security Center Web Console se deben volver a generar mediante el instalador.

# Deshabilitar Identity and Access Manager

Si lo desea, puede deshabilitar Identity and Access Manager (también conocido como IAM).

*Para deshabilitar IAM, haga lo siguiente:*

1. En el menú principal, vaya a **Configuración → Integración**.
2. En la sección **Identity and Access Manager**, deshabilite el botón de **Identity and Access Manager**.

   Puede habilitar IAM en cualquier momento más tarde.

Si actualiza Kaspersky Security Center Web Console a través del instalador y especifica que no desea instalar IAM, Kaspersky Security Center Web Console se actualiza y IAM no se instala. Toda la información sobre la integración con Kaspersky Industrial CyberSecurity for Networks se eliminará del dispositivo, así como los archivos de configuración de IAM y los archivos de registro.

# Configurar la autenticación de dominio mediante los protocolos NTLM y Kerberos

Kaspersky Security Center 15.1 permite utilizar la autenticación de dominio en OpenAPI mediante los protocolos NTLM y Kerberos. El uso de la autenticación de dominio le permite a un usuario de Windows habilitar la autenticación segura en Kaspersky Security Center Web Console sin tener que volver a ingresar la contraseña en la red corporativa (inicio de sesión único).

La autenticación de dominio en OpenAPI sobre el protocolo Kerberos tiene las siguientes restricciones:

- El usuario de Kaspersky Security Center Web Console se debe autenticar en Active Directory mediante el protocolo Kerberos. El usuario debe tener un Ticket Granting Ticket de Kerberos válido (también conocido como TGT). Un TGT se emite automáticamente cuando se autentifica en el dominio.

- Debe configurar la autenticación Kerberos en el navegador. Para obtener más información, consulte la documentación del navegador que esté utilizando.

Si desea utilizar la autenticación de dominio mediante los protocolos Kerberos, su red debe cumplir con las siguientes condiciones:

- El Servidor de administración debe ejecutarse con el nombre de cuenta del dominio.

- El servidor de Kaspersky Security Center Web Console se debe instalar en el mismo dispositivo donde está instalado el Servidor de administración.

- Debe especificar los siguientes Nombres principales de servicio (SPN) para la cuenta del Servidor de administración:

  - "http/<server.fqnd.name>"

  - "http/<server>"

  Aquí <servidor> es el nombre de red del Servidor de administración y <server.fqnd.name> es el nombre de dominio completo (FQDN) del dispositivo del Servidor de administración.

- Al conectarse con la Consola de administración o con Kaspersky Security Center Web Console, la dirección del Servidor de administración debe especificarse exactamente como la dirección para la que está registrado el Nombre principal de servicio (SPN). Puede especificar <server.fqnd.name> o <server>.

- Para un inicio de sesión sin contraseña, el proceso del navegador en el que se abre Kaspersky Security Center Web Console como navegador debe ejecutarse con una cuenta de dominio.

Los protocolos Kerberos y NTLM solo son compatibles con OpenAPI para Kaspersky Security Center 15.1. No son compatibles con OpenAPI para Kaspersky Security Center Linux.

# Configuración del Servidor de administración

Esta sección describe el proceso de configuración y las propiedades del Servidor de administración de Kaspersky Security Center.

# Configuración de la conexión de Kaspersky Security Center Web Console al Servidor de administración

*Para configurar los puertos de conexión del Servidor de administración:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la ficha **General**, seleccione la sección **Puertos de conexión**.

La aplicación muestra la configuración de conexión principal del servidor seleccionado.

La Consola de administración está conectada al Servidor de administración a través del puerto SSL TCP 13299. Los objetos de automatización klakaut pueden utilizar este mismo puerto.

El puerto TCP 14000 se puede utilizar para conectar la Kaspersky Security Center Web Console, los puntos de distribución, los Servidores de administración secundarios y los objetos de automatización klakaut, así como para recibir datos desde dispositivos cliente.

Normalmente, el puerto SSL TCP 13000 solo puede ser utilizado por el Agente de red, un Servidor de administración secundario y el Servidor de administración principal en DMZ. En algunos casos, es posible que Kaspersky Security Center Web Console deba conectarse mediante el puerto SSL 13000:

- Si se prefiere usar un solo puerto SSL tanto para Kaspersky Security Center Web Console como para otras actividades (recepción de datos desde dispositivos cliente, conexión de puntos de distribución o conexión de Servidores de administración secundarios).
- Si un objeto de automatización klakaut no se conecta al Servidor de administración directamente, sino mediante un punto de distribución en DMZ.

# Configurar el registro de eventos de conexiones del Servidor de administración

El historial de conexiones e intentos de conexión con el Servidor de administración durante su funcionamiento se puede guardar en un archivo de registro. La información en el archivo le permite rastrear no solo las conexiones desde su infraestructura de red, sino también los intentos no autorizados de acceder al servidor.

*Para registrar los eventos de conexión al Servidor de administración:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la ficha **General**, seleccione la sección **Puertos de conexión**.

3. Habilitar la opción **Registrar eventos de conexiones del Servidor de administración**.

Todos los eventos adicionales de la conexión con el Servidor de administración, los resultados de autenticación y los errores de SSL se guardarán en el archivo %ProgramData%\KasperskyLab\adminkit\logs\SC.syslog.

# Configuración de las opciones de acceso a Internet para el Servidor de administración

Debe configurar el acceso a Internet para usar Kaspersky Security Network y descargar actualizaciones y bases de datos antivirus para Kaspersky Security Center y las aplicaciones de Kaspersky administradas.

*Para especificar la configuración de acceso a Internet para el Servidor de administración:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, seleccione la sección **Configuración de acceso a Internet**.

3. Active la opción **Usar servidor proxy** si quiere usar un servidor proxy al conectarse a Internet. Si activa esta opción, los campos estarán disponibles para ingresar ajustes. Deberá introducir los siguientes valores de conexión del servidor proxy:

   - **Dirección**

     Dirección del servidor proxy usado para conectar Kaspersky Security Center con Internet.

   - **Número de puerto**

     Número del puerto a través del cual se establecerá la conexión proxy de Kaspersky Security Center.

   - **No usar el servidor proxy para direcciones locales**

     Ningún servidor proxy se usará para conectarse a los dispositivos en la red local.

   - **Autenticación del servidor proxy**

     Si se selecciona esta casilla, en los campos de entrada se podrán especificar las credenciales para la autenticación del servidor proxy.

     Este campo de entrada está disponible cuando la casilla **Usar servidor proxy** está desmarcada.

   - **Nombre de usuario**

     Cuenta de usuario con la que se establece la conexión al servidor proxy (este campo está disponible si se selecciona la casilla **Autenticación del servidor proxy**).

   - **Contraseña**

     Contraseña que especifica el usuario con cuya cuenta se establece la conexión al servidor proxy (este campo está disponible si se selecciona la casilla **Autenticación del servidor proxy**).

     Para ver la contraseña indicada, mantenga presionado el botón **Mostrar** durante la cantidad de tiempo que sea necesario.

También puede configurar el acceso a Internet mediante el asistente de inicio rápido.

# Configuración del número máximo de eventos en el repositorio de eventos

En la sección **Repositorio de eventos** de la ventana de propiedades del Servidor de administración, puede editar la configuración del almacenamiento de eventos en la base de datos del Servidor de administración limitando el número de registros de eventos o el tiempo de almacenamiento de los registros. Cuando se especifica el número máximo de eventos, la aplicación calcula una cantidad aproximada de espacio de almacenamiento requerido para el número especificado. Puede utilizar este cálculo aproximado para evaluar si tiene suficiente espacio libre en el disco para evitar el desbordamiento de la base de datos. La capacidad predeterminada de la base de datos del Servidor de administración es de 400 000 eventos. La capacidad máxima recomendada de la base de datos es de 45 millones de eventos.

La aplicación comprueba la base de datos cada 10 minutos. Si la cantidad de eventos alcanza el valor máximo especificado más 10 000, la aplicación elimina los eventos más antiguos para que solo quede la cantidad máxima de eventos especificada.

Cuando el Servidor de administración elimina los eventos antiguos, no puede guardar los nuevos eventos en la base de datos. Durante este período de tiempo, la información sobre los eventos que fueron rechazados se escribe en el Registro de eventos de Kaspersky. Los nuevos eventos se ponen en cola y se guardan en la base de datos una vez finalizada la operación de borrado.

*Para limitar la cantidad de eventos que se pueden almacenar en el repositorio de eventos en el Servidor de administración:*

1. En el menú principal, haga clic en el ícono de configuración (  ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la ficha **General**, seleccione la sección **Repositorio de eventos**. Especifique el número máximo de eventos almacenados en la base de datos.

3. Haga clic en el botón **Guardar**.

Además, puede hacer lo siguiente:

- Cambiar la configuración de cualquier tarea para guardar eventos relacionados con el progreso de la misma, o guardar solo los resultados de la ejecución de la tarea.

- Reducir o deshabilitar el período de almacenamiento para los eventos del Servidor de administración, el Agente de red y las aplicaciones de Kaspersky instaladas en los dispositivos administrados.

Al hacerlo, reducirá la cantidad de eventos en la base de datos, aumentará la velocidad de ejecución de los escenarios asociados con el análisis de la tabla de eventos en la base de datos y disminuirá el riesgo de que una gran cantidad de eventos sobrescriban eventos críticos.

# Configuración de conexión de dispositivos con protección de UEFI

El *Dispositivo con protección de UEFI* es un dispositivo que tiene una aplicación o solución de Kaspersky para UEFI integrada al nivel de BIOS. La protección integrada garantiza que el dispositivo está protegido desde el momento en que se lo enciende. La protección en dispositivos sin software integrado, por el contrario, no comienza a funcionar sino hasta que la aplicación de seguridad se inicia. Kaspersky Security Center admite la administración de estos dispositivos.

*Para modificar la configuración de conexión de los dispositivos con protección de UEFI, realice lo siguiente:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, seleccione **Puertos adicionales**.

3. Modifique la configuración relevante:

   - **Abrir puerto para dispositivos con protección de UEFI y dispositivos con KasperskyOS**

     Los dispositivos con protección de UEFI podrán conectarse al Servidor de administración.

   - **Puerto para dispositivos con protección de UEFI y dispositivos con KasperskyOS**

     Puede cambiar el número de puerto si la opción **Abrir puerto para dispositivos con protección de UEFI y dispositivos con KasperskyOS** está habilitada. El número de puerto predeterminado es 13294.

4. Haga clic en el botón **Guardar**.

Los dispositivos con protección de UEFI pueden conectarse ahora al Servidor de administración.

# Creación de una jerarquía de servidores de administración: agregar un Servidor de administración secundario

## Agregado del Servidor de administración secundario (realizado en el futuro Servidor de administración principal)

Puede agregar un Servidor de administración como Servidor de administración secundario, estableciendo así una jerarquía "principal/secundario".

*Para agregar un Servidor de administración secundario al que sea posible conectarse mediante Kaspersky Security Center Web Console:*

1. Asegúrese de que el puerto 13000 del futuro Servidor de administración principal esté disponible para la recepción de conexiones desde los Servidores de administración secundarios.
2. En el futuro Servidor de administración principal, haga clic en el ícono de configuración ( ).
3. En la página de propiedades que se abre, seleccione la pestaña **Servidores de administración**.
4. Seleccione la casilla de verificación junto al nombre del grupo de administración al que desea agregar el Servidor de administración.
5. En la línea del menú, haga clic en **Conectar Servidor de administración secundario**.

   Se inicia el Asistente para agregar un Servidor de administración secundario. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
6. Complete los siguientes campos:

   - **Conectar el Servidor de administración principal a un Servidor de administración secundario en DMZ**

     Seleccione esta opción si el Servidor de administración secundario está en una zona desmilitarizada (DMZ).

     Si se selecciona esta opción, debe especificar el parámetro **Dirección del Servidor secundario**.

     Si se selecciona esta opción, el Servidor de administración principal inicia la conexión con el Servidor de administración secundario. En caso contrario, el Servidor de administración secundario inicia la conexión con el Servidor de Administración primario.

   - **Nombre para mostrar del Servidor de administración secundario**

     Un nombre para identificar al Servidor de administración secundario en la jerarquía. Puede usar, por ejemplo, la dirección IP del Servidor o una frase como "Servidor secundario para el grupo 1".

   - **Dirección del Servidor de administración secundario (opcional)**

     Escriba la dirección IP o el nombre de dominio del Servidor de administración secundario.

     Este parámetro es necesario si la opción **Conectar el Servidor de administración principal al Servidor de administración secundario en DMZ** está habilitada.

   - **Puerto SSL del Servidor de administración**

     Especifique el número del puerto de SSL en el Servidor de administración principal. El número de puerto predeterminado es 13000.

   - **Puerto de la API del Servidor de administración**

     Especifique el número del puerto en el Servidor de administración principal para recibir conexiones de OpenAPI. El número de puerto predeterminado es 13299.

7. Especifique el certificado del Servidor de administración secundario. Si especificó el parámetro **Dirección del Servidor secundario**, puede hacer clic en el botón **Obtener del Servidor de administración secundario** para obtener el certificado. De lo contrario, haga clic en el botón **Buscar el archivo de certificado** y localice el archivo de certificado.

8. Configure los ajustes de conexión:

   - Introduzca la dirección del futuro Servidor de administración principal.

   - Si el futuro Servidor de administración secundario usa un servidor proxy, ingrese la dirección del servidor proxy y las credenciales de usuario para conectarse al servidor proxy.

9. Ingrese las credenciales de un usuario que tenga derechos para acceder al futuro Servidor de administración secundario.

10. Si la verificación en dos pasos está habilitada y configurada, especifique el código de seguridad generado por la app de autenticación.

    Si la verificación en dos pasos está habilitada pero no configurada para la cuenta que especifica, debe crear la jerarquía desde el futuro Servidor secundario (consulte las instrucciones a continuación).

Si los ajustes de conexión son correctos, se establecerá la conexión con el futuro Servidor secundario y se creará la jerarquía principal-secundario. Si la conexión no se puede establecer, revise los ajustes de conexión o especifique el certificado del futuro Servidor secundario manualmente.

La conexión entre los Servidores de administración principal y secundario se establece a través del puerto 13000. Se recibirán y aplicarán las tareas y directivas del Servidor de administración principal. El Servidor de administración secundario aparecerá en el Servidor de administración principal, en el grupo de administración en el que se lo haya agregado.

## Agregado del Servidor de administración secundario (realizado en el futuro Servidor de administración secundario)

Si no pudo conectarse al futuro Servidor de administración secundario (por ejemplo, debido a que se desconectó temporalmente o no estaba disponible para la conexión), aún puede agregar un Servidor de administración secundario.

*Para agregar un Servidor de administración como secundario que no se pueda conectar mediante Kaspersky Security Center Web Console:*

1. Envíe el archivo de certificado del futuro Servidor de administración principal al administrador del sistema de la oficina donde se encuentra el futuro Servidor de administración secundario (por ejemplo, puede escribir el archivo en un dispositivo externo, como una unidad flash o enviarlo por correo electrónico).

   El archivo de certificado se encuentra en el futuro Servidor de administración principal, en %ALLUSERSPROFILE %\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

2. Solicite al administrador del sistema a cargo del futuro Servidor de administración secundario que haga lo siguiente:

   a. Haga clic en el ícono de configuración ( ).

   b. En la página de propiedades que se abre, vaya a la sección **Jerarquía de Servidores de administración** de la pestaña **General**.

   c. Seleccione la opción **Este Servidor de administración es un servidor secundario en la jerarquía**.

   d. En el campo **Dirección del Servidor de administración principal**, ingrese el nombre de red del Servidor de administración principal futuro.

   e. Seleccione el archivo guardado anteriormente con el certificado del futuro Servidor de administración principal haciendo clic en **Examinar**.

   f. De ser necesario, seleccione la casilla **Conectar el Servidor de administración principal a un Servidor de administración secundario en DMZ**.

   g. Si la conexión con el futuro Servidor de administración secundario se realiza a través de un servidor proxy, seleccione la opción **Usar servidor proxy** y especifique la configuración de la conexión.

   h. Haga clic en **Guardar**.

Así se constituye la jerarquía "principal/secundario". El Servidor de administración principal comienza a recibir conexiones del Servidor de administración secundario utilizando el puerto 13000. Se recibirán y aplicarán las tareas y directivas del Servidor de administración principal. El Servidor de administración secundario se muestra en el Servidor de administración principal, en el grupo de administración donde se agregó.

# Ver la lista de servidores de administración secundarios

*Para ver la lista de los Servidores de administración secundarios (incluido el virtual), haga lo siguiente:*

En el menú principal, haga clic en el nombre del Servidor de administración, ubicado junto al ícono de configuración ( ).

Se muestra una lista desplegable con el nombre de los servidores de administración secundarios (incluidos los virtuales).

Haga clic en alguno de los nombres para interactuar con el Servidor de administración correspondiente.

Los grupos de administración también se muestran, pero aparecen en gris y no están disponibles para su administración en este menú.

Si está conectado a su Servidor de administración principal en Kaspersky Security Center Web Console y no puede conectarse a un Servidor de administración virtual administrado por un Servidor de administración secundario, puede usar una de las siguientes estrategias:

- Modifique la instalación de Kaspersky Security Center Web Console para agregar el servidor secundario a la lista de servidores de administración de confianza. Una vez que haga esto, podrá conectarse al Servidor de administración virtual en Kaspersky Security Center Web Console.

  1. En el dispositivo en el que haya instalado Kaspersky Security Center Web Console, ejecute el archivo ksc-web-console-<número de versión>.<número de compilación>.exe. Utilice para esto una cuenta con privilegios administrativos.

     Se iniciará el asistente de instalación. Avance por el asistente utilizando el botón **Siguiente**.

  2. Seleccione la opción **Actualizar**.

  3. En el paso **Tipo de modificación**, seleccione la opción **Editar la configuración de conexión**.

  4. En el paso **Servidores de administración de confianza**, agregue el Servidor de administración secundario necesario.

  5. En el último paso, haga clic en **Modificar** para aplicar la nueva configuración.

  6. Cuando la aplicación se haya reconfigurado, haga clic en el botón **Finalizar**.

- Use Kaspersky Security Center Web Console para conectarse directamente al Servidor de administración secundario en el que se haya creado el servidor virtual. Una vez que haga esto, podrá cambiar al Servidor de administración virtual en Kaspersky Security Center Web Console.

- Utilice la consola de administración basada en MMC para conectarse directamente al servidor virtual.

# Eliminar una jerarquía de servidores de administración

Si ya no desea tener una jerarquía de servidores de administración, puede desconectar los servidores de la jerarquía.

*Para eliminar una jerarquía de servidores de administración:*

1. En el menú principal, haga clic en el ícono de Configuración ( ) ubicado junto al nombre del Servidor de administración principal.

2. En la página que se abre, vaya a la pestaña **Servidores de administración**.

3. Busque el grupo de administración al que pertenezca el servidor de administración secundario que desee eliminar y seleccione ese servidor.

4. En la línea del menú, haga clic en **Eliminar**.

5. En la ventana que se abre, haga clic en **Aceptar** para confirmar que desea eliminar el Servidor de administración secundario.

El Servidor de administración que supo actuar como principal y el Servidor de administración que supo actuar como secundario se vuelven independientes. La jerarquía deja de existir.

# Mantenimiento del Servidor de administración

El mantenimiento del Servidor de administración permite liberar espacio en la carpeta del Servidor de administración y reducir el volumen de las bases de datos al eliminar objetos que ya no son necesarios. Esto lo ayuda a mejorar el rendimiento y la fiabilidad del funcionamiento de la aplicación. Le recomendamos realizar un mantenimiento del Servidor de administración por lo menos una vez a la semana.

El mantenimiento del Servidor de administración se lleva a cabo a través de la tarea especializada. La aplicación realiza las acciones siguientes durante el mantenimiento del Servidor de administración:

- Elimina carpetas y archivos innecesarios de la carpeta de almacenamiento.
- Elimina los registros innecesarios de las tablas (también conocidos como "referencias colgantes").
- Borra la caché.
- Mantiene las bases de datos (si usa SQL Server o PostgreSQL como DBMS):
  - Comprueba las bases de datos en busca de errores (disponible solo para SQL Server).
  - Reorganiza los índices de la base de datos.
  - Actualiza las estadísticas de la base de datos.
  - Reduce la base de datos si es necesario.

La tarea Mantenimiento del Servidor de administración se crea automáticamente al instalar Kaspersky Security Center. Si ha eliminado la tarea Mantenimiento del Servidor de administración, puede crearla otra vez manualmente.

*Para crear una Mantenimiento del Servidor de administración:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.

2. Haga clic en el botón **Agregar**.

   Se inicia el Asistente para crear nueva tarea.

3. En la ventana **Configuración de tarea nueva** del Asistente, seleccione **Mantenimiento del Servidor de administración** como tipo de tarea y haga clic en el botón **Siguiente**.

4. Siga el resto de instrucciones del asistente.

Encontrará la nueva tarea en la lista de tareas. Solo puede haber una tarea Mantenimiento del Servidor de administración en ejecución por cada Servidor de administración. Si creó creado una tarea Mantenimiento del Servidor de administración para un Servidor de administración, no podrá crear una nueva tarea Mantenimiento del Servidor de administración.

# Configuración de la interfaz

Puede configurar la interfaz de Kaspersky Security Center Web Console para mostrar u ocultar distintas secciones y elementos de interfaz según las funciones que utilice.

*Para configurar la interfaz de Kaspersky Security Center Web Console y adaptarla a las características que utilice:*

1. En el menú principal, vaya a la configuración de su cuenta y, a continuación, seleccione **Opciones de interfaz.**
2. En la ventana **Opciones de interfaz** que se abre, habilite o deshabilite las opciones obligatorias.
3. Haga clic en **Guardar**.

   Luego, la consola muestra secciones en el menú principal de acuerdo con las opciones habilitadas. Por ejemplo, si habilita **Mostrar alertas EDR**, la sección **Supervisión e informes** → **Alertas** aparece en el menú principal.

# Administración de servidores de administración virtuales

En esta sección, se describen las siguientes acciones para administrar Servidores de administración virtuales.

- Crear Servidores de administración virtual
- Habilitar y deshabilitar Servidores de administración virtual
- Asignar un administrador para un Servidor de administración virtual
- Cambiar el Servidor de administración de los dispositivos cliente
- Eliminar Servidores de administración virtual

## Crear un Servidor de administración virtual

Puede crear servidores de administración virtuales y agregarlos a grupos de administración.

Cuando crea un Servidor de administración virtual, hereda la lista de usuarios y todos los derechos de usuario del Servidor de administración principal. Si un usuario tiene derechos de acceso al Servidor principal, este usuario también tiene derechos de acceso al Servidor virtual. Después de la creación, usted configura los derechos de acceso a los servidores de forma independiente.

*Para crear y agregar un Servidor de administración virtual:*

1. En el menú principal, haga clic en el icono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.
2. En la página que se abre, vaya a la pestaña **Servidores de administración**.

3. Seleccione el grupo de administración al que quiere agregar el Servidor de administración virtual.
   El Servidor de administración virtual administrará los dispositivos que pertenezcan al grupo seleccionado (o a los subgrupos de ese grupo).

4. En la línea del menú, haga clic en **Nuevo Servidor de administración virtual**.

5. En la página que se abre, defina las propiedades del nuevo Servidor de administración virtual:

   - **Nombre del Servidor de administración virtual**.
   - **Dirección de conexión con el Servidor de administración**

     Puede usar el nombre o la dirección IP del Servidor de administración.

6. En la lista de usuarios, seleccione al administrador del Servidor de administración virtual. Si lo desea, puede editar una de las cuentas existentes antes de asignarle la función de administrador o crear una nueva cuenta de usuario.

7. Haga clic en **Guardar**.

Se crea el nuevo Servidor de administración virtual y se lo agrega al grupo de administración seleccionado. El nuevo Servidor aparecerá en la pestaña **Servidores de administración**.

Si está conectado a su Servidor de administración principal en Kaspersky Security Center Web Console y no puede conectarse a un Servidor de administración virtual administrado por un Servidor de administración secundario, puede usar una de las siguientes estrategias:

- Modifique la instalación de Kaspersky Security Center Web Console para agregar el servidor secundario a la lista de servidores de administración de confianza. Una vez que haga esto, podrá conectarse al Servidor de administración virtual en Kaspersky Security Center Web Console.

  1. En el dispositivo en el que haya instalado Kaspersky Security Center Web Console, ejecute el archivo ksc-web-console-<número de versión>.<número de compilación>.exe. Utilice para esto una cuenta con privilegios administrativos.

     Se iniciará el asistente de instalación. Avance por el asistente utilizando el botón **Siguiente**.

  2. Seleccione la opción **Actualizar**.

  3. En el paso **Tipo de modificación**, seleccione la opción **Editar la configuración de conexión**.

  4. En el paso **Servidores de administración de confianza**, agregue el Servidor de administración secundario necesario.

  5. En el último paso, haga clic en **Modificar** para aplicar la nueva configuración.

  6. Cuando la aplicación se haya reconfigurado, haga clic en el botón **Finalizar**.

- Use Kaspersky Security Center Web Console para conectarse directamente al Servidor de administración secundario en el que se haya creado el servidor virtual. Una vez que haga esto, podrá cambiar al Servidor de administración virtual en Kaspersky Security Center Web Console.

- Utilice la consola de administración basada en MMC para conectarse directamente al servidor virtual.

# Habilitación y deshabilitación de un Servidor de administración virtual

Si crea un nuevo Servidor de administración virtual, quedará habilitado por defecto. Puede habilitarlo y deshabilitarlo en cualquier momento. Habilitar y deshabilitar un Servidor de administración virtual equivale a encender y apagar un Servidor de administración físico.

*Para habilitar o deshabilitar un Servidor de administración virtual:*

1. En el menú principal, haga clic en el icono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.
2. En la página que se abre, vaya a la pestaña **Servidores de administración**.
3. Seleccione el Servidor de administración virtual que desee habilitar o deshabilitar.
4. En la línea del menú, haga clic en el botón **Habilitar/deshabilitar el Servidor de administración virtual**.

   Dependiendo del estado que tuviera antes de esta acción, el Servidor de administración virtual cambiará de estado a habilitado o deshabilitado. El nuevo estado aparecerá junto al nombre del Servidor de administración.

# Asignar un administrador para un Servidor de administración virtual

Cuando utiliza Servidores de administración virtuales en su organización, es posible que desee asignar un administrador dedicado para cada Servidor de administración virtual. Esto puede ser útil, por ejemplo, cuando una organización crea servidores virtuales para administrar oficinas o departamentos separados o cuando un proveedor de servicios administrados (MSP) desea administrar sus inquilinos a través de servidores virtuales.

Cuando crea un Servidor de administración virtual, hereda la lista de usuarios y todos los derechos de usuario del Servidor de administración principal. Si un usuario tiene derechos de acceso al Servidor principal, este usuario también tiene derechos de acceso al Servidor virtual. Después de la creación, usted configura los derechos de acceso a los servidores de forma independiente. Si desea asignar un administrador solo para un Servidor de administración virtual, asegúrese de que el administrador no tenga derechos de acceso en el Servidor de administración principal.

Asigna un administrador para un Servidor de administración virtual otorgando al administrador derechos de acceso al Servidor de administración virtual. Puede otorgar los derechos de acceso necesarios de una de las siguientes maneras:

- Configure los derechos de acceso para el administrador manualmente
- Asigne uno o más roles de usuario para el administrador

Para iniciar sesión en Kaspersky Security Center Web Console, el administrador de un Servidor de administración virtual ingresa el nombre del Servidor de administración virtual y su nombre de usuario y contraseña. Kaspersky Security Center Web Console autentica al administrador y abre el Servidor de administración virtual al que el administrador está autorizado a acceder. El administrador no puede cambiar entre Servidores de Administración.

## Requisitos previos

Antes de comenzar, asegúrese de que se cumplan las siguientes condiciones:

- Se crea el Servidor de administración virtual.
- En el Servidor de administración principal, creó una cuenta para el administrador que desea asignar para el Servidor de administración virtual.
- Tiene el derecho **Modificar ACL de objeto** en el área funcional **Características generales → Permisos de usuario**.

## Configurar derechos de acceso manualmente

*Para asignar un administrador para un Servidor de administración virtual:*

1. En el menú principal, cambie al Servidor de administración virtual pertinente:
   a. Haga clic en el ícono de corchete (›) a la derecha del nombre del Servidor de administración actual.
   b. Seleccione el Servidor de administración requerido.
2. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración.
   Se abre la ventana Propiedades del Servidor de administración.
3. En la pestaña **Derechos de acceso**, haga clic en el botón **Agregar**
   Se abre una lista unificada de usuarios del Servidor de administración principal y el Servidor de administración virtual actual.
4. En la lista de usuarios, seleccione la cuenta del administrador que desea asignar para el Servidor de administración virtual y, a continuación, haga clic en el botón **Aceptar**.
   La aplicación agrega el usuario seleccionado a la lista de usuarios en la pestaña **Derechos de acceso**.
5. Marque la casilla ubicada junto a la cuenta agregada y haga clic en el botón **Derechos de acceso**.
6. Configure los derechos que tendrá el administrador sobre el Servidor de administración virtual.
   Para una autenticación correcta, el administrador debe tener, por lo menos, los siguientes derechos:
   - Derecho de **Leer** en el área funcional **Características generales → Funcionalidad básica**
   - Derecho de **Leer** en el área funcional **Características generales → Servidores de administración virtuales**

La aplicación guarda los derechos de usuario modificados en la cuenta de administrador.

## Configurar derechos de acceso mediante la asignación de roles de usuario

Como alternativa, puede otorgar los derechos de acceso a un administrador del Servidor de administración virtual a través de roles de usuario. Por ejemplo, esto podría ser útil si desea asignar varios administradores en el mismo Servidor de administración virtual. Si este es el caso, puede asignar a las cuentas de los administradores la misma o más roles de usuario en lugar de configurar los mismos derechos de usuario para varios administradores.

*Para asignar un administrador para un Servidor de administración virtual mediante la asignación de roles de usuario:*

1. En el Servidor de administración principal, cree un nuevo rol de usuario y, a continuación, especifique todos los derechos de acceso necesarios que un administrador debe tener en el Servidor de administración virtual. Puede crear varios roles, por ejemplo, si desea separar el acceso a diferentes áreas funcionales.

2. En el menú principal, cambie al Servidor de administración virtual pertinente:

   a. Haga clic en el ícono de corchete (›) a la derecha del nombre del Servidor de administración actual.

   b. Seleccione el Servidor de administración requerido.

3. Asigne el nuevo rol o varios roles a la cuenta de administrador.

La aplicación asigna los roles a la cuenta del administrador.

### Configuración de derechos de acceso al nivel de objeto

Además de asignar derechos de acceso al nivel de área funcional, puede configurar el acceso a objetos específicos en el Servidor de administración virtual, por ejemplo, a un grupo de administración específico o una tarea. Para hacer esto, cambie al Servidor de administración virtual y, a continuación, configure los derechos de acceso en las propiedades del objeto.

## Cambiar los dispositivos cliente de Servidor de administración

Se puede cambiar el Servidor de administración que administra los dispositivos cliente por otro con la tarea *Cambiar Servidor de administración*. Cuando se completa esta tarea, los dispositivos cliente seleccionados quedan bajo el mando del Servidor de administración elegido.

No se puede utilizar la tarea *Cambiar Servidor de administración* para dispositivos cliente conectados al Servidor de administración a través de puertas de enlace de conexión. Para estos dispositivos, debe reconfigurar el Agente de red o reinstalar el Agente de red y especificar la puerta de enlace de conexión.

*Para cambiar el Servidor de administración que administra ciertos dispositivos cliente:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.

2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. En el paso **Configuración de tarea nueva** del asistente, especifique estos ajustes:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Security Center**.

   b. En el campo **Tipo de tarea**, seleccione **Cambiar Servidor de administración**.

   c. En la ventana **Nombre de la tarea**, póngale un nombre a la tarea que está creando.

   El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).

   d. Seleccione los dispositivos a los que se asignará la tarea.

   - Asignar tarea a un grupo de administración

     La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

     Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

     Si la tarea se asigna a un grupo de administración, la pestaña **Seguridad** no se mostrará en la ventana de propiedades de la tarea; esto se debe a que las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

   - Especificar las direcciones de los dispositivos manualmente o importarlas de una lista

     Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

     Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.

   - Asignar tarea a una selección de dispositivos

     La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

     Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

4. En el paso **Alcance de la tarea** del asistente, especifique un grupo de administración, dispositivos con direcciones específicas o una selección de dispositivos.

5. En este paso del asistente, confirme que acepta las condiciones de cambio del Servidor de administración para dispositivos cliente.

6. En el siguiente paso del asistente, seleccione el Servidor de administración que desea utilizar para administrar los dispositivos seleccionados:

- Cambiar a otro Servidor de administración principal

  Para mover dispositivos cliente a otro servidor de administración principal, especifique los siguientes ajustes de conexión del servidor de administración:

  1. En el campo **Dirección del Servidor de administración**, especifique la dirección del nuevo servidor de administración principal.
  2. En el campo **Número de puerto**, especifique el número de puerto para conectarse al Servidor de administración.

     El número de puerto predeterminado es 14000.
  3. Especifique el número del **Puerto SSL** en el Servidor de administración principal.

     El número de puerto predeterminado es 13000.
  4. De ser necesario, active la opción **Usar servidor proxy**.

     Si esta opción está desactivada, se utiliza la conexión directa para conectar el dispositivo al Servidor de administración.

     Si esta opción está habilitada, especifique los parámetros del servidor proxy:

     - **Dirección del servidor proxy**
     - **Puerto del servidor proxy**

     Si su servidor proxy requiere autenticación, en los campos **Nombre de usuario** y **Contraseña**, especifique las credenciales de la cuenta con la cual se establece la conexión con el servidor proxy. Le recomendamos que utilice las credenciales de una cuenta que solamente tenga los privilegios mínimos necesarios para completar la autenticación ante el servidor proxy.
  5. Si es necesario, cargue un nuevo certificado del Servidor de Administración.

- Cambiar a otro Servidor virtual en este Servidor principal

  Seleccione esta opción para mover los dispositivos cliente al Servidor de administración virtual en el Servidor de administración principal actual. Para ello, en la lista desplegable **Nombre del Servidor de administración virtual**, seleccione el Servidor de administración virtual necesario.

7. En el paso **Seleccione una cuenta con la que ejecutar la tarea** del asistente, especifique la configuración de la cuenta:

   - **Cuenta predeterminada**

     La tarea se ejecutará utilizando la misma cuenta que la aplicación que realizará la tarea.

     Esta opción está seleccionada de forma predeterminada.

   - **Especificar cuenta**

     Complete los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta con la que se ejecutará la tarea. La cuenta debe tener los derechos necesarios para realizar la tarea.

     - **Cuenta**

       Cuenta con la que se ejecutará la tarea.

     - **Contraseña**

       Contraseña de la cuenta con la que se ejecutará la tarea.

8. Si desea cambiar la configuración predeterminada de la tarea, en el paso **Finalizar la creación de la tarea** del asistente, active la opción **Abrir los detalles de la tarea cuando se complete la creación**.

   Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Puede cambiar la configuración por defecto más tarde, en cualquier momento.

9. Haga clic en el botón **Finalizar**.

   Se crea la tarea y se la agrega a la lista de tareas.

10. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.

11. Si desea cambiar la configuración predeterminada de la tarea, en la ventana de propiedades de la tarea, especifique la configuración general de la tarea según sus necesidades.

12. Haga clic en el botón **Guardar**.

    La tarea queda creada y configurada.

13. Ejecute la tarea creada.

Una vez que se completa la tarea, los dispositivos cliente para los que se la creó quedan bajo el mando del Servidor de administración especificado en la configuración de la tarea.

## Eliminación de un Servidor de administración virtual

Si elimina un Servidor de administración virtual, se eliminarán también todos los objetos que se hayan creado en el mismo, incluidas las directivas y las tareas. Los dispositivos administrados que pertenezcan a los grupos de administración controlados por el Servidor de administración virtual serán eliminados de esos grupos. Para volver a administrar esos dispositivos con Kaspersky Security Center, deberá realizar un sondeo de red y mover los dispositivos del grupo Dispositivos no asignados a los grupos de administración que desee.

*Para eliminar un Servidor de administración virtual:*

1. En el menú principal, haga clic en el icono de configuración ( ) ubicado junto al nombre del Servidor de administración.
2. En la página que se abre, vaya a la pestaña **Servidores de administración**.
3. Seleccione el Servidor de administración virtual que desee eliminar.
4. En la línea del menú, haga clic en el botón **Eliminar**.

Se elimina el Servidor de administración virtual.

# Habilitación de la protección de una cuenta desde la modificación no autorizada

Puede habilitar una opción adicional para proteger la cuenta de un usuario contra modificaciones no autorizadas. Si esta opción está habilitada, la modificación de la configuración de la cuenta de usuario requiere la autorización del usuario con derechos de modificación.

*Para habilitar o deshabilitar la protección de una cuenta desde la modificación no autorizada:*

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios**.
2. Haga clic en el nombre de la cuenta de usuario interna para la que desea especificar la protección de la cuenta frente a modificaciones no autorizadas.
3. En la ventana que se abre con los ajustes del usuario, seleccione la pestaña **Protección de cuentas**.
4. En la pestaña **Protección de cuentas**, seleccione la opción **Solicitar autenticación para comprobar el permiso de modificación de las cuentas de usuario** si desea solicitar las credenciales cada vez que se cambie o modifique la configuración de la cuenta. De lo contrario, seleccione la opción **Permitir a los usuarios modificar esta cuenta sin autenticación adicional**.
5. Haga clic en el botón **Guardar**.

La protección de la cuenta contra modificaciones no autorizadas está habilitada para una cuenta de usuario.

# Copia de seguridad y restauración de los datos del Servidor de administración

La copia de seguridad de datos le permite mover un Servidor de administración de un dispositivo a otro, sin pérdida de datos. Mediante la copia de seguridad, puede restaurar datos al mover las bases de datos del Servidor de Administración a otro dispositivo o al actualizar a una versión más nueva de Kaspersky Security Center. Además, puede usar la copia de seguridad de datos para mover datos del Servidor de Administración desde Kaspersky Security Center Windows y ponerlos bajo la administración de Kaspersky Security Center Linux (no se admite mover datos de Kaspersky Security Center Linux a Kaspersky Security Center Windows).

No se realiza una copia de seguridad de los complementos de administración instalados. Después de restaurar los datos del Servidor de administración a partir de una copia de seguridad, debe descargar y volver a instalar los complementos para las aplicaciones administradas.

Antes de crear una copia de seguridad de los datos del Servidor de administración, verifique si se agregó un Servidor de administración virtual al grupo de administración. Si se agrega un Servidor de administración virtual, asegúrese de que se asigne un administrador a este Servidor de administración virtual antes de realizar la copia de seguridad. No puede otorgar derechos de acceso de administrador al Servidor de administración virtual después de la copia de seguridad. Tenga en cuenta que si se pierden las credenciales de la cuenta de administrador, no podrá asignar un nuevo administrador al Servidor de administrador virtual.

Para hacer un respaldo o restaurar un clúster de conmutación por error de Kaspersky Security Center, debe detener todo el clúster para realizar el mantenimiento y, luego, reiniciarlo cuando se complete el respaldo o la restauración.

Puede crear una copia de seguridad de los datos del Servidor de administración mediante uno de los siguientes métodos:

- Al crear y ejecutar una tarea de copia de seguridad de datos utilizando la Consola de administración.
- Puede ejecutar la utilidad klbackup en el dispositivo que tiene instalado el Servidor de administración. Esta utilidad está incluida en el kit de distribución de Kaspersky Security Center. Una vez instalado el Servidor de administración, la encontrará en la raíz de la carpeta de destino especificada durante la instalación de la aplicación.

Se guardan los siguientes datos en la copia de seguridad del Servidor de administración:

- Base de datos del Servidor de administración (directivas, tareas, parámetros de la aplicación, eventos guardados en el Servidor de administración).
- Información de configuración de la estructura de los grupos de administración y los dispositivos cliente.
- Repositorio de paquetes de distribución de aplicaciones para instalación remota.

- Certificado del Servidor de administración.
- Contenido de la carpeta *Actualizaciones*.

  De forma predeterminada, la ruta de la carpeta es C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\

La restauración de los datos del Servidor de administración solo se puede realizar mediante la utilidad klbackup. Para llevar a cabo la restauración en una instancia del Servidor de administración que se acaba de instalar, que esté en funcionamiento y que sea de la misma versión para la que se haya creado la copia de seguridad (o de una versión más reciente).

## Creación de una tarea de copia de seguridad de datos

Las tareas de copia de seguridad son tareas del Servidor de administración y se crean a través del asistente de inicio rápido. Si se elimina una tarea de copia de seguridad creada por el asistente de inicio rápido, puede crearse otra manualmente.

*Para crear una tarea de copia de seguridad de los datos del Servidor de administración:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en el botón **Agregar**.

   Se inicia el Asistente para crear nueva tarea.
3. En la ventana **Configuración de tarea nueva** del Asistente, seleccione el tipo de tarea denominado **Copia de seguridad de los datos del Servidor de administración**.
4. Siga el resto de instrucciones del asistente.

Solo puede crear una única copia de la tarea **Copia de seguridad de los datos del Servidor de administración**. Si la tarea de copia de seguridad de los datos del Servidor de administración ya fue creada para el Servidor de administración, no se mostrará en la ventana de selección del tipo de tarea del Asistente de creación de tareas de copia de seguridad.

*Para configurar la tarea Copia de seguridad de los datos del Servidor de administración:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas** y, luego, seleccione la tarea **Copia de seguridad de los datos del Servidor de administración**.
2. Haga clic en la tarea **Copia de seguridad de los datos del Servidor de administración**.

   Se abrirá la ventana de propiedades de la tarea.
3. Si es necesario, especifique la configuración general de la tarea de acuerdo con sus necesidades.
4. En la sección **Configuración de la aplicación**, especifique la ruta a la carpeta para almacenar las copias de seguridad de los datos del Servidor de administración, establezca la contraseña de protección de la copia de seguridad y la cantidad de copias de seguridad si es necesario.
5. Haga clic en **Guardar** para aplicar los cambios.

Se configura la tarea *Copia de seguridad de los datos del Servidor de administración*.

# Mover el Servidor de administración a otro dispositivo

Si necesita usar el Servidor de administración en un nuevo dispositivo, puede moverlo de una de las siguientes maneras:

- Mueva el Servidor de administración y el servidor de la base de datos a un nuevo dispositivo (el servidor de la base de datos se puede instalar en el nuevo dispositivo junto con el Servidor de administración, o en otro dispositivo).
- Mantenga el servidor de la base de datos en el dispositivo anterior y mueva solo el Servidor de administración a un nuevo dispositivo.

*Para mover el Servidor de administración y el servidor de la base de datos a un nuevo dispositivo:*

1. En el dispositivo anterior, cree una copia de seguridad de los datos del Servidor de administración.

   Para ello, inicie la tarea de copia de seguridad de datos a través de Kaspersky Security Center Web Console o ejecute la utilidad klbackup.

   > Habilite esta opción si el Servidor de administración utiliza SQL Server como DBMS y usted desea migrar los datos de SQL Server a un DBMS MySQL o MariaDB. Para hacer esto, ejecute la utilidad klbackup en modo interactivo para crear una copia de seguridad de los datos. Habilite la opción **Migrar al formato de MySQL/MariaDB** en el la ventana **Opciones de copia de seguridad** del asistente de copias de seguridad y restauración. Kaspersky Security Center creará una copia de seguridad compatible con MySQL y MariaDB. Podrá restaurar los datos de esa copia en MySQL o MariaDB.

   > También puede habilitar la opción **Migrar al formato de Azure** si desea migrar los datos de SQL Server a Azure SQL DBMS.

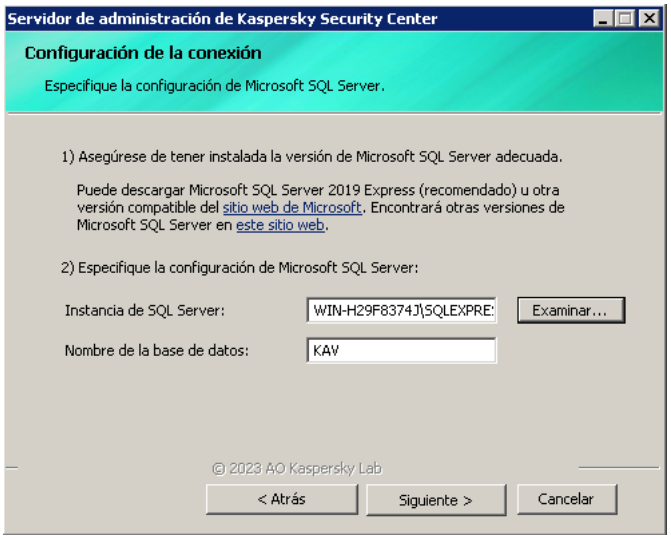
2. En el dispositivo anterior, desconecte el Servidor de administración de la red.
3. Seleccione un nuevo dispositivo para instalar el Servidor de administración. Asegúrese de que el hardware y el software del dispositivo seleccionado cumplan con los requisitos del Servidor de administración, Kaspersky Security Center Web Console y Agente de red. Además, compruebe que haya puertos utilizados en el Servidor de administración disponibles.
4. Asigne la misma dirección al nuevo dispositivo.

   Al nuevo Servidor de Administración se le puede asignar un nombre NetBIOS, un FQDN y una dirección IP estática. Esto depende de la dirección del Servidor de administración que se haya configurado en el paquete de instalación del Agente de red cuando se desplegaron los agentes de red. Como alternativa, puede usar la dirección de conexión que determina el Servidor de administración al que se conecta el Agente de red (puede obtener esta dirección en los dispositivos administrados mediante la utilidad klnagchk).
5. Si es necesario, instale en otro dispositivo el sistema de administración de base de datos (DBMS) que utilizará el Servidor de administración.

   La base de datos se puede instalar en el nuevo dispositivo junto con el Servidor de administración o en otro dispositivo. Cerciórese de que este dispositivo cumpla con los requisitos de hardware y software. Cuando seleccione un DBMS, tenga en cuenta la cantidad de dispositivos cubiertos por el Servidor de administración.

6. Ejecute la instalación del Servidor de administración en el nuevo dispositivo.

7. Durante la instalación del Servidor de administración, configure los parámetros de conexión del servidor de la base de datos.




Ejemplo de la ventana de configuración de conexión para Microsoft SQL Server

Dependiendo de dónde necesite ubicar el servidor de la base de datos, realice una de las siguientes acciones:

- Mantenga el servidor de la base de datos en el dispositivo anterior

  1. Haga clic en el botón **Examinar** junto al campo **Instancia de SQL Server** y seleccione el nombre del dispositivo anterior en la lista que aparece.

     Tenga en cuenta que el dispositivo anterior debe estar disponible para la conexión con el nuevo Servidor de Administración.

  2. Introduzca el nombre de la base de datos anterior en el campo **Nombre de la base de datos**.

- Mueva el servidor de la base de datos a otro dispositivo

  1. Haga clic en el botón **Examinar** junto al campo **Instancia de SQL Server** y seleccione el nuevo nombre del dispositivo en la lista que aparece.

  2. Introduzca el nuevo nombre de la base de datos en el campo **Nombre de la base de datos**.

     Tenga en cuenta que el nuevo nombre de la base de datos debe coincidir con el nombre de la base de datos del dispositivo anterior. Los nombres de las bases de datos deben ser idénticos para que se pueda utilizar la copia de seguridad del Servidor de administración. El nombre predeterminado de la base de datos es *KAV*.

8. Una vez completada la instalación, recupere los datos del Servidor de administración en el nuevo dispositivo mediante la utilidad klbackup.

Si utiliza SQL Server como DBMS en los dispositivos anteriores y nuevos, tenga en cuenta que la versión de SQL Server instalada en el dispositivo nuevo debe ser igual o posterior a la versión de SQL Server instalada en el dispositivo anterior. De lo contrario, no podrá recuperar los datos del Servidor de administración en el dispositivo nuevo.

9. Abra Kaspersky Security Center Web Console y conéctese al Servidor de administración.
10. Verifique que todos los dispositivos administrados estén conectados al Servidor de administración.
11. Desinstale el Servidor de administración y el servidor de la base de datos del dispositivo anterior.

También puede usar la Consola de administración para mover el Servidor de administración y un servidor de bases de datos a otro dispositivo.

# Comprobar la integridad de los módulos mediante las utilidades klscmodchk e Integrity_checker

Kaspersky Security Center contiene varios módulos binarios en forma de bibliotecas de enlace dinámico, archivos ejecutables, archivos de configuración y archivos de interfaz. Los intrusos pueden reemplazar uno o más módulos ejecutables o archivos de aplicación con otros archivos que contengan códigos maliciosos. Para prevenir la sustitución de módulos y archivos, Kaspersky Security Center ofrece verificar la integridad de los componentes mediante las utilidades klscmodchk e integrity_checker. Estas utilidades comprueban los módulos y archivos en busca de cambios no autorizados o daños. Si un módulo o archivo de aplicación tiene una suma de control incorrecta, se considera dañado.

La utilidad klscmodchk comprueba la integridad de los siguientes componentes de Kaspersky Security Center:

- Servidor de administración
- Agente de red
- Complementos de administración para la Consola de administración con archivos de manifiesto

La utilidad integrity_checker comprueba la integridad de los siguientes componentes de Kaspersky Security Center:

- Servidor de administración
- Agente de red
- Kaspersky Security Center Web Console

Ambas utilidades comprueban la integridad del módulo aplicando el archivo de manifiesto kl_file_integrity_manifest.xml, que es parte de la compilación de Kaspersky Security Center y se encuentra en la carpeta de instalación. El archivo de manifiesto del componente contiene archivos cuya integridad es importante para el correcto funcionamiento del componente de Kaspersky Security Center. También se comprueba la integridad de los archivos de manifiesto.

Se recomienda no modificar el archivo de manifiesto kl_file_integrity_manifest.xml, ya que esto invalidará la firma digital y hará que la comprobación de integridad falle.

Para comprobar la integridad del componente de Kaspersky Security Center, ejecute uno de los siguientes comandos:

- `$ klscmodchk [ parámetros ]`

  La utilidad klscmodchk inicia la utilidad integrity_checker con el parámetro `--verbose` y verifica la integridad de los módulos.

  Parámetros de la utilidad klscmodchk:

  - `-logfile <log_file_path>`: especifica la ruta a un archivo en el disco para el registro. De forma predeterminada, la información se envía a la consola.
  - `-chkplugins`: comprobar la integridad de los módulos del complemento de administración instalados en la Consola de administración que incluyen archivos de manifiesto. De forma predeterminada, los complementos de administración no se analizan.
  - `-verbose`: muestra información ampliada durante la comprobación de integridad.

- `$ integrity_checker [ parámetros ] <ruta_del_archivo_de_manifiesto>`

  Parámetros de la utilidad integrity_checker:

  - `--help`: muestra la ayuda de la utilidad integrity_checker.
  - `--version`: muestra la versión de la utilidad integrity_checker.
  - `--verbose`: muestra información sobre el funcionamiento de la utilidad. Al realizar una comprobación de integridad, es suficiente usar este parámetro en el comando.

El resultado de la verificación de cada archivo de manifiesto se muestra junto al nombre del archivo de manifiesto en el siguiente formato:

- SUCCEEDED: integridad del archivo confirmada (código de retorno 0).
- FAILED: integridad del archivo no confirmada (código de retorno diferente de cero).

También puede configurar las comprobaciones de integridad para que se inicien automáticamente al iniciar la aplicación. De manera predeterminada, la verificación de integridad automática está deshabilitada.

*Para habilitar la verificación de integridad automática:*

1. En el dispositivo donde está instalado el Servidor de administración, en el símbolo del sistema de Windows, ingrese el siguiente comando:

   ```
   klscflag.exe -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. Reiniciar el dispositivo.

La verificación de integridad automática está habilitada.

En la próxima ejecución de Kaspersky Security Center, la utilidad klscmodchk se ejecutará junto con el Servidor de administración e iniciará la verificación de la integridad de los módulos. El resultado de las verificaciones de integridad se escribe en el Registro de eventos de Kaspersky.

# Configuración inicial de Kaspersky Security Center Web Console

En esta sección, se describen los pasos que debe seguir tras instalar Kaspersky Security Center Web Console para realizar su configuración inicial.

## Asistente de inicio rápido (Kaspersky Security Center Web Console)

Esta sección proporciona información acerca del Asistente de inicio rápido del Servidor de administración.

El Asistente requiere acceso a Internet. Si su Servidor de administración no tiene acceso a Internet, le recomendamos que realice todos los pasos del Asistente de forma manual, a través de la interfaz de Kaspersky Security Center Web Console.

Kaspersky Security Center le permite ajustar una selección mínima de parámetros de configuración para crear un sistema centralizado de administración para proteger su red contra amenazas de seguridad. La configuración de estos ajustes se realiza a través del asistente de inicio rápido. Cuando el asistente se está ejecutando, le permite hacer los siguientes cambios en la aplicación:

- Agregar archivos de clave o introducir códigos de activación que puedan distribuirse automáticamente a los dispositivos de los grupos de administración.
- Configurar la interacción con Kaspersky Security Network (KSN). Si se permitió el uso de KSN, el Asistente habilita el servicio del Servidor proxy de KSN, que garantiza la conexión entre KSN y los dispositivos.
- Configura la entrega mediante correo electrónico de notificaciones de eventos que ocurren durante la operación del Servidor de administración y las aplicaciones administradas (para garantizar la entrega de una notificación exitosa, el servicio de Messenger debe ejecutarse en el Servidor de administración y en todos los dispositivos de destino).
- Crear una directiva de protección para estaciones de trabajo y servidores, además de tareas de análisis antimalware, tareas de descarga de actualizaciones y tareas de copia de seguridad de datos, para el nivel superior de la jerarquía de dispositivos administrados.

  El asistente de inicio rápido únicamente crea directivas para aquellas aplicaciones que no tienen una directiva en su carpeta **Dispositivos administrados**. El asistente de inicio rápido no crea tareas si detecta tareas con el mismo nombre creadas para el nivel más alto de la jerarquía de dispositivos administrados.

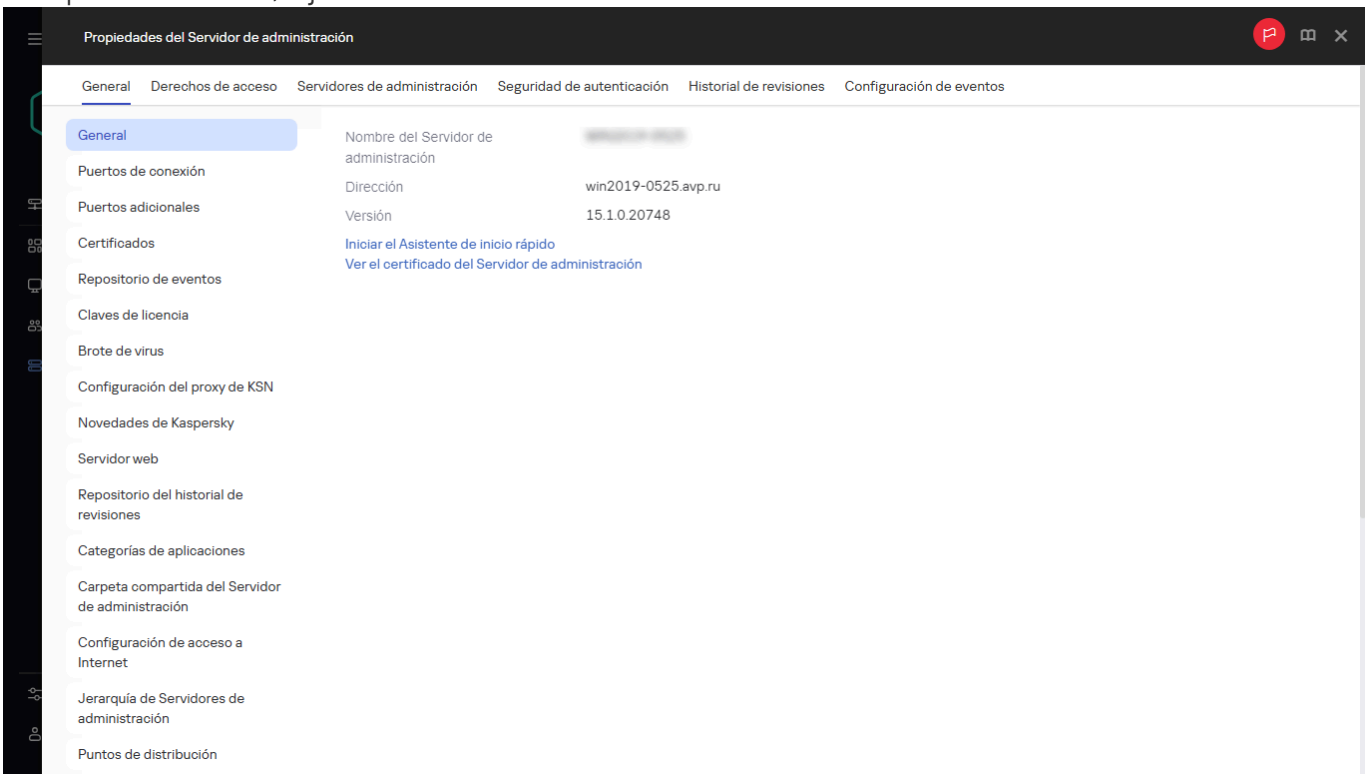
La aplicación le preguntará si desea abrir el asistente de inicio rápido cuando termine con la instalación del Servidor de administración y se conecte a este por primera vez. El asistente de inicio rápido también se puede ejecutar manualmente en cualquier momento.

*Para iniciar el asistente de inicio rápido manualmente:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **General**.



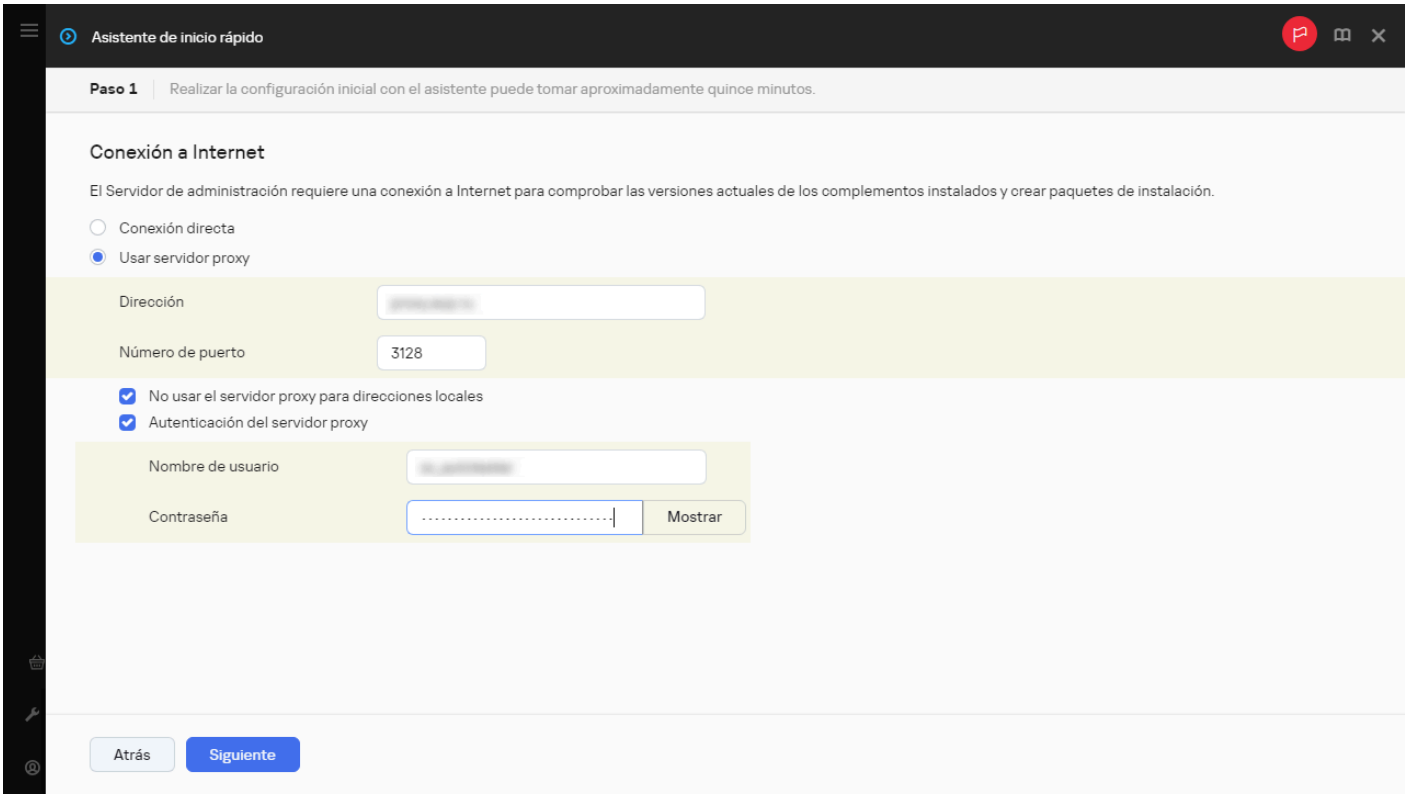

Ventana de propiedades del Servidor de administración

3. Haga clic en **Iniciar el Asistente de inicio rápido**.

El asistente le ofrecerá realizar la configuración inicial del Servidor de administración. Siga las instrucciones del asistente. Avance por el asistente utilizando el botón **Siguiente**.

# Paso 1. Especificar la configuración de la conexión a Internet

Especifique la configuración de acceso a Internet para el Servidor de administración. Debe configurar el acceso a Internet para usar Kaspersky Security Network y descargar actualizaciones y bases de datos antivirus para Kaspersky Security Center y las aplicaciones de Kaspersky administradas.




Configuración de la conexión a Internet

Active la opción **Usar servidor proxy** si quiere usar un servidor proxy al conectarse a Internet. Si activa esta opción, los campos estarán disponibles para ingresar ajustes. Deberá introducir los siguientes valores de conexión del servidor proxy:

- Dirección

  Dirección del servidor proxy usado para conectar Kaspersky Security Center con Internet.

- Número de puerto

  Número del puerto a través del cual se establecerá la conexión proxy de Kaspersky Security Center.

- No usar el servidor proxy para direcciones locales

  Ningún servidor proxy se usará para conectarse a los dispositivos en la red local.

- Autenticación del servidor proxy

  Si se selecciona esta casilla, en los campos de entrada se podrán especificar las credenciales para la autenticación del servidor proxy.

  Este campo de entrada está disponible cuando la casilla **Usar servidor proxy** está desmarcada.

- Nombre de usuario

  Cuenta de usuario con la que se establece la conexión al servidor proxy (este campo está disponible si se selecciona la casilla **Autenticación del servidor proxy**).

- Contraseña

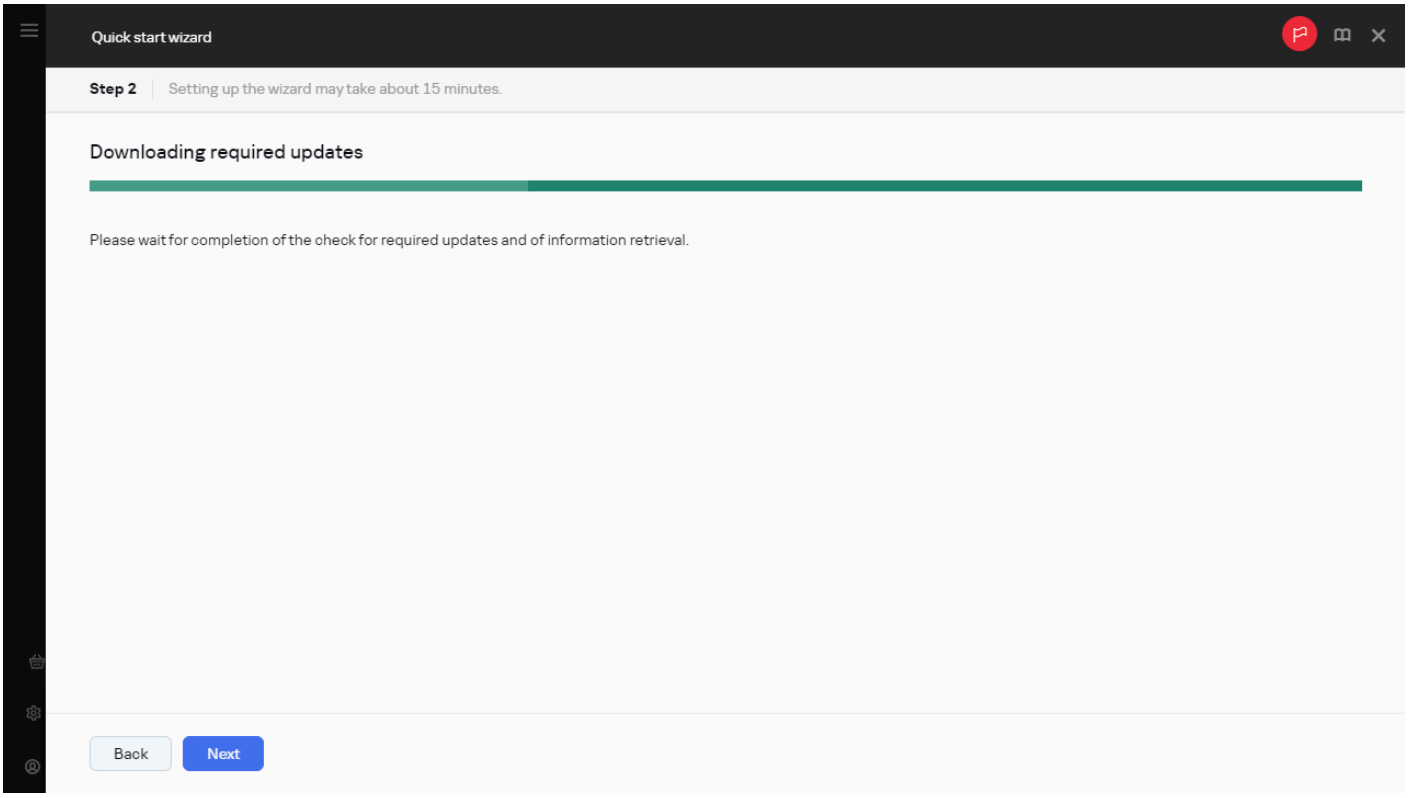
  Contraseña que especifica el usuario con cuya cuenta se establece la conexión al servidor proxy (este campo está disponible si se selecciona la casilla **Autenticación del servidor proxy**).

  Para ver la contraseña indicada, mantenga presionado el botón **Mostrar** durante la cantidad de tiempo que sea necesario.

Puede configurar el acceso a Internet más tarde, sin usar el asistente de inicio rápido.

## Paso 2. Descargando actualizaciones requeridas

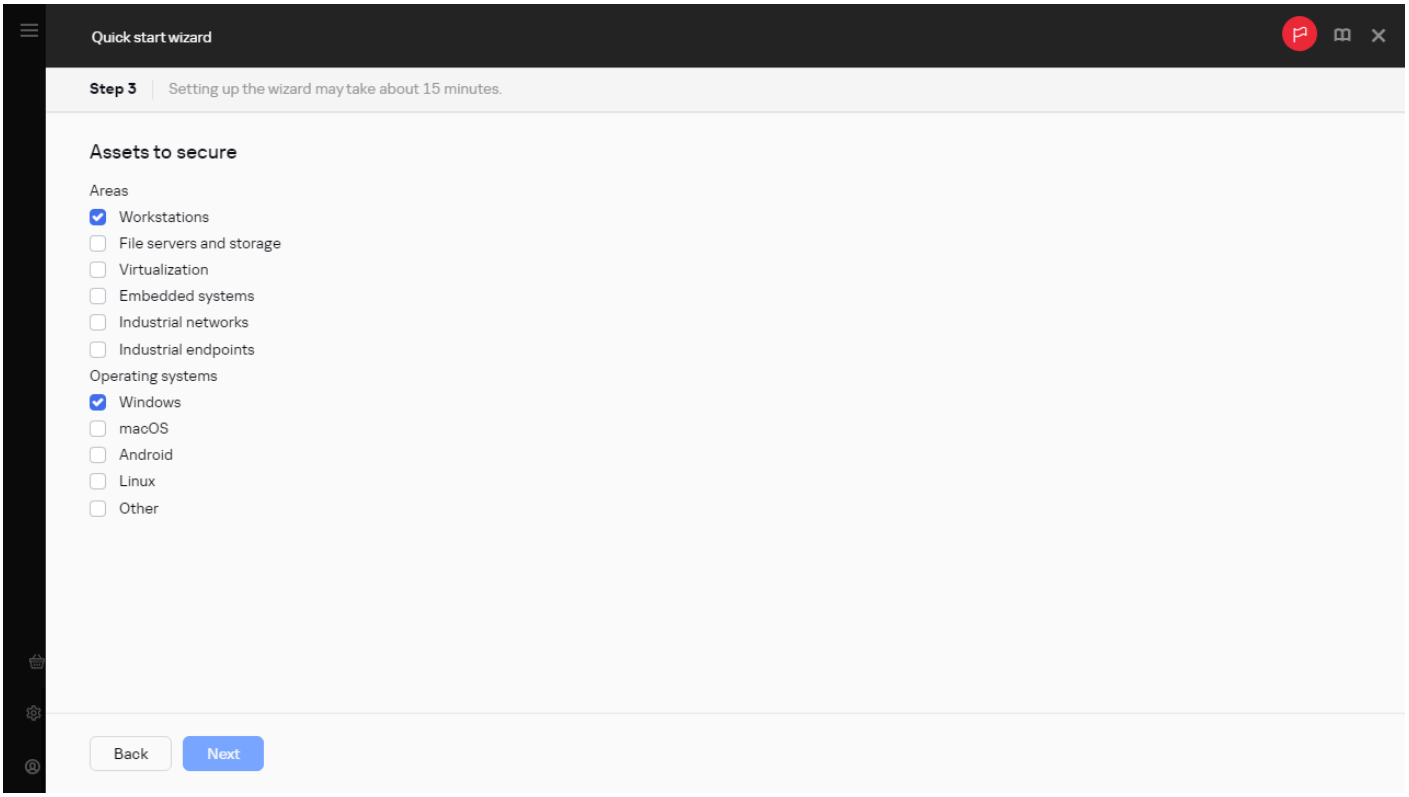
Las actualizaciones necesarias se descargan de los servidores de Kaspersky automáticamente.




Descargando actualizaciones requeridas

# Paso 3. Selección de los activos para asegurar

Seleccione las áreas que desee proteger y los sistemas operativos que estén presentes en su red. Cuando selecciona estas opciones, especifica los filtros para los complementos de administración de aplicaciones y los paquetes de distribución en los servidores de Kaspersky que puede descargar para instalar en los dispositivos cliente en su red.




Selección de los activos para asegurar

Seleccione las opciones:

- **Áreas**

  Puede elegir las siguientes áreas de protección:

  - **Estaciones de trabajo**. Seleccione esta opción si desea proteger las estaciones de trabajo en su red. La estación de trabajo está seleccionada de forma predeterminada.
  - **Servidores de archivos y almacenamiento**. Seleccione esta opción si desea proteger los servidores de archivos en su red.
  - **Dispositivos móviles**. Seleccione esta opción si desea proteger los dispositivos móviles pertenecientes a la empresa o a los empleados de la empresa. Si selecciona esta opción pero no indica una licencia con la función de Administración de dispositivos móviles, aparecerá un mensaje en el que se le solicita que brinde una licencia con la función de Administración de dispositivos móviles. Si no brinda una licencia, no puede utilizar la función de dispositivos móviles.
  - **Virtualización**. Seleccione esta opción si desea proteger las máquinas virtuales en su red.
  - **Kaspersky Antispam**. Seleccione esta opción si desea proteger los servidores de correos electrónicos de su organización contra el correo no deseado, el fraude y la entrega de malware.
  - **Sistemas integrados**. Seleccione esta opción si desea proteger los sistemas integrados basados en Windows, como los cajeros automáticos (ATM).
  - **Redes industriales**. Seleccione esta opción si desea monitorear los datos de seguridad en su red industrial y desde los endpoints de la red que están protegidos por las aplicaciones de Kaspersky.
  - **Endpoints industriales**. Seleccione esta opción si desea proteger nodos virtuales individuales dentro de una red industrial.

- **Sistemas operativos**

  Puede seleccionar las siguientes plataformas:

  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - Otro

  Para obtener información sobre los sistemas operativos compatibles, consulte la sección Requisitos de hardware y software para Kaspersky Security Center Web Console.

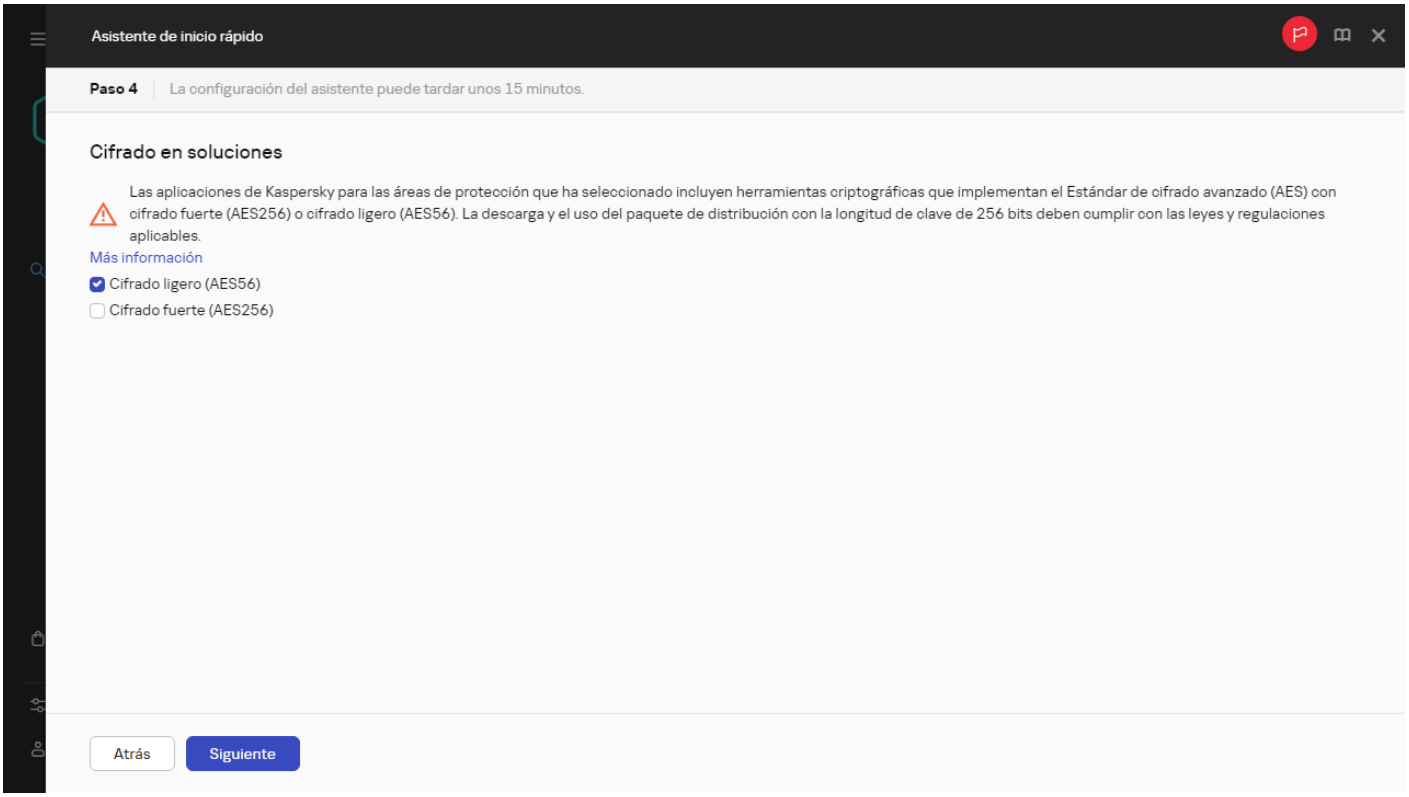
Puede seleccionar los paquetes de aplicaciones de Kaspersky de la lista de paquetes disponibles más adelante, sin usar el asistente de inicio rápido. Para ayudarse a encontrar los paquetes necesarios, puede filtrar la lista de paquetes disponibles utilizando una serie de criterios.

# Paso 4. Seleccionar el cifrado en las soluciones

La ventana **Cifrado en soluciones** aparecerá únicamente si ha seleccionado **Estaciones de trabajo** como área de protección.

Kaspersky Endpoint Security para Windows incluye herramientas para cifrar la información almacenada en dispositivos cliente con Windows. Estas herramientas implementan el estándar de cifrado avanzado AES, con una longitud de clave de 256 o 56 bits.

El paquete de distribución con una longitud de clave de 256 bits solo puede descargarse y utilizarse si lo permiten las leyes y normativas en vigor. Para descargar un paquete de distribución de Kaspersky Endpoint Security para Windows que se adecue a las necesidades de su organización, consulte la legislación del país en el que se encuentren los dispositivos cliente de su organización.




Seleccionar el cifrado en las soluciones

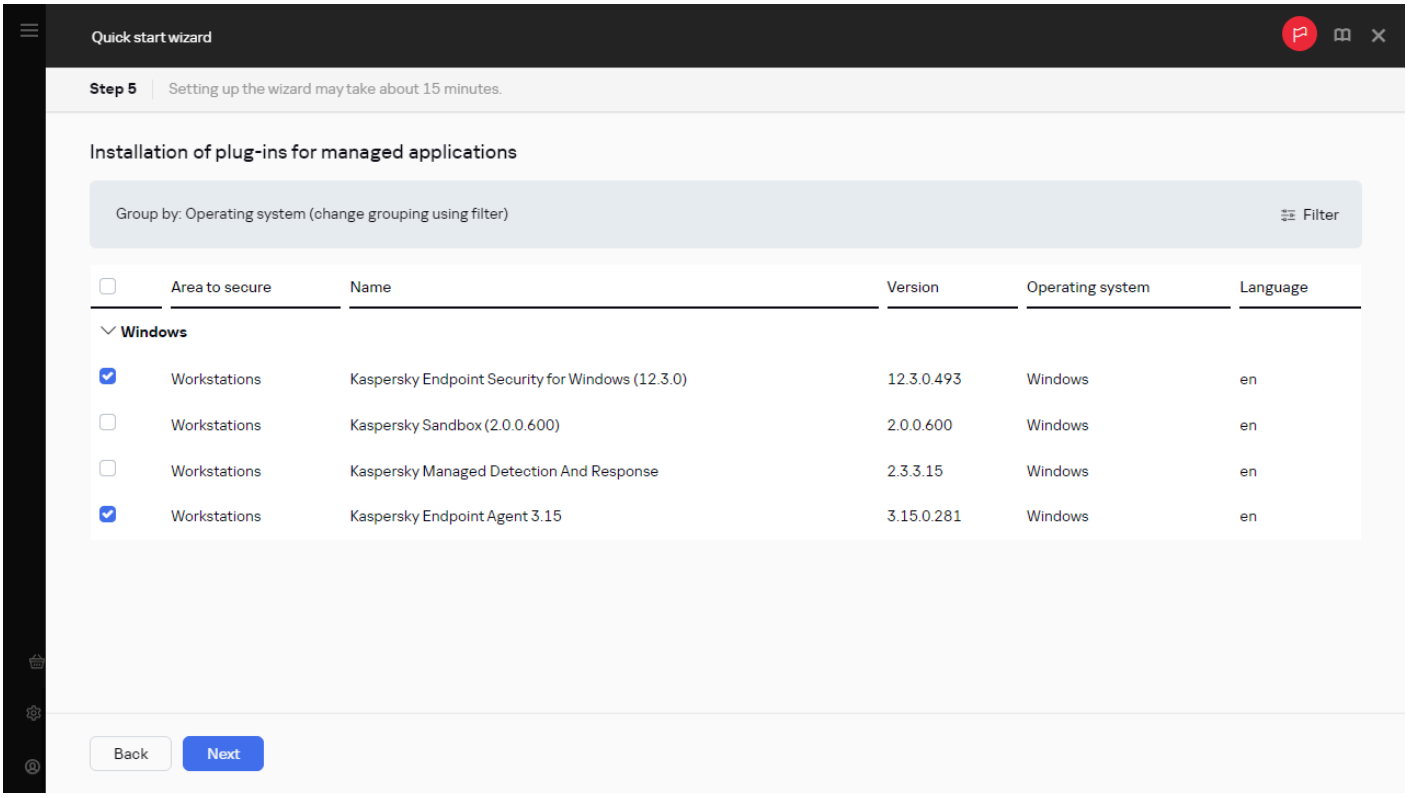
En la ventana **Cifrado en soluciones**, seleccione uno de los siguientes tipos de cifrado:

- Cifrado ligero. Este tipo de cifrado utiliza una longitud de clave de 56 bits.
- Cifrado fuerte. Este tipo de cifrado utiliza una longitud de clave de 256 bits.

Puede seleccionar el paquete de distribución para Kaspersky Endpoint Security for Windows con el tipo de cifrado requerido más adelante, independientemente del asistente de inicio rápido.

# Paso 5. Configurar la instalación de los complementos para las aplicaciones administradas

Seleccione los complementos para aplicaciones administradas que se instalarán. Se muestra una lista de complementos ubicados en los servidores de Kaspersky. La lista tendrá aplicado un filtro basado en las opciones seleccionadas en el paso anterior del asistente. Por defecto, una lista completa incluye complementos de todos los idiomas. Para mostrar solo el complemento de un idioma específico, utilice el filtro.




Instalación de complementos para aplicaciones administradas

La lista de complementos incluye las siguientes columnas:

- **Área para proteger**

  Las áreas seleccionadas para protección se muestran en esta columna.

- **Tipo**

  Los tipos de complementos se muestran en esta columna.

- **Nombre**

  Estarán seleccionados los complementos que dependan de los componentes y las plataformas que haya seleccionado en el paso anterior.

- **Versión**

  La lista incluye complementos de todas las versiones colocadas en los servidores de Kaspersky. De forma predeterminada, se seleccionan los complementos de las últimas versiones.

- **Versión más reciente**

  Esta columna indica si la versión del complemento es la más reciente. Si se muestra el valor **true**, el complemento correspondiente tiene la versión más reciente instalada. Si se muestra el valor **false**, el complemento correspondiente tiene una versión posterior.

- **Sistema operativo**

  Esta columna muestra los sistemas operativos de los complementos.

- **Idioma**

  De forma predeterminada, el idioma de localización de un complemento está definido por el idioma de Kaspersky Security Center que ha seleccionado en la instalación. Puede especificar otros idiomas en la lista desplegable **Mostrar el idioma de localización de la Consola de administración o**.

Una vez seleccionados los complementos, haga clic en **Siguiente** para iniciar la instalación.

Puede instalar complementos de administración para aplicaciones Kaspersky manualmente, por separado del asistente de inicio rápido.

El asistente de inicio rápido instala automáticamente los complementos seleccionados. Para instalar algunos complementos, debe aceptar los términos del EULA. Lea el texto de EULA que se muestra, seleccione la casilla de verificación **Acepto utilizar Kaspersky Security Network** y haga clic en el botón **Instalar**. Si no acepta los términos del EULA, el complemento no se instala.

Cuando todos los complementos seleccionados se hayan instalado, el asistente de inicio rápido avanzará automáticamente al paso siguiente.

## Paso 6. Instalando los complementos seleccionados

El asistente de inicio rápido instalará automáticamente los complementos seleccionados en el paso anterior. Para instalar algunos complementos, debe aceptar los términos del EULA. Lea el texto de EULA que se muestra, seleccione la casilla de verificación **Acepto utilizar Kaspersky Security Network** y haga clic en el botón **Instalar**. Si no acepta los términos del EULA, el complemento no se instala.

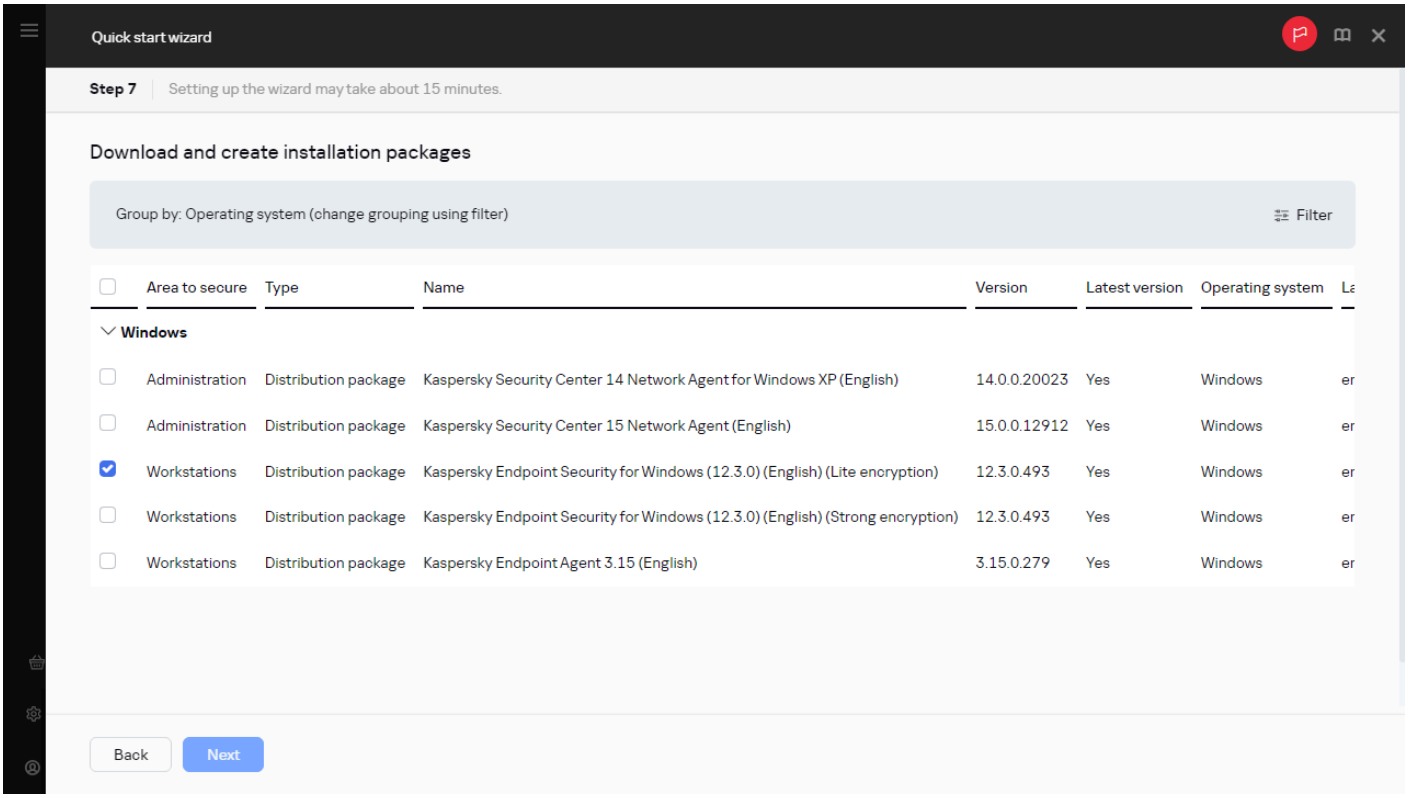
Cuando todos los complementos seleccionados se hayan instalado, el asistente de inicio rápido avanzará automáticamente al paso siguiente.

# Paso 7. Descarga de paquetes de distribución y creación de paquetes de instalación

Seleccione los paquetes de distribución que desea descargar.

Los paquetes de distribución de las aplicaciones administradas pueden requerir que la versión de Kaspersky Security Center instalada no sea anterior a una versión en particular.

Después de seleccionar un tipo de cifrado para Kaspersky Endpoint Security para Windows, se muestra una lista de paquetes de distribución de ambos tipos de cifrado. El paquete de distribución que corresponda al tipo de cifrado elegido estará seleccionado en dicha lista. Puede seleccionar los paquetes de distribución de cualquier tipo de cifrado. El idioma del paquete de distribución corresponde al idioma de Kaspersky Security Center. Si no existe un paquete de distribución de Kaspersky Endpoint Security para Windows para el idioma de Kaspersky Security Center, se selecciona el paquete de distribución en inglés.




Descarga de paquetes de distribución y creación de paquetes de instalación

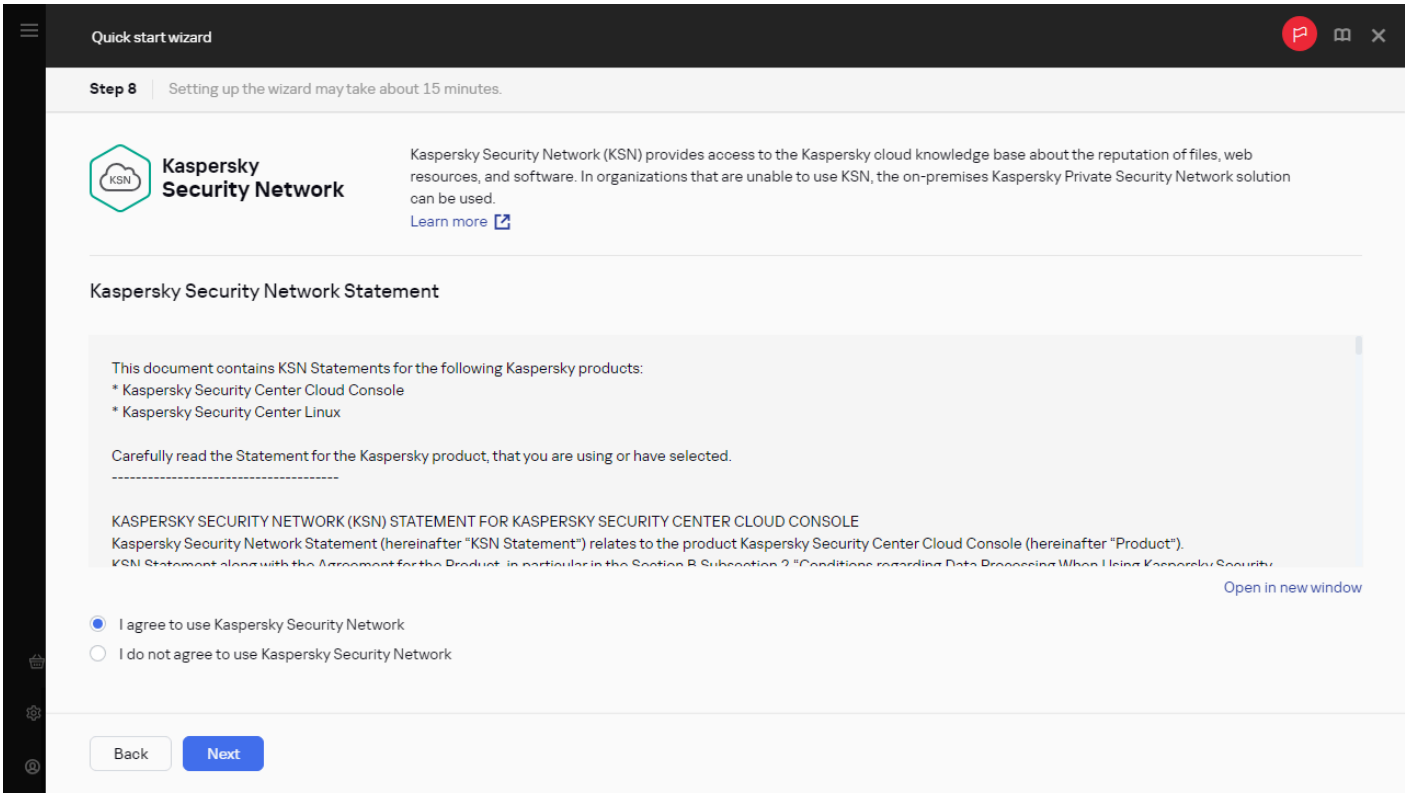
Para finalizar la descarga de algunos paquetes de distribución, debe aceptar el EULA. Cuando hace clic en el botón **Aceptar**, se muestra el texto de EULA. Para avanzar al siguiente paso del asistente, debe aceptar los términos y condiciones del EULA y los términos y condiciones de la Política de privacidad de Kaspersky. Si no acepta los términos y condiciones, se cancela la descarga del paquete.

Después de haber aceptado los términos y condiciones del EULA y los términos y condiciones de la Política de privacidad de Kaspersky, la descarga de los paquetes de distribución continúa. Más tarde, podrá usar paquetes de instalación para desplegar las aplicaciones de Kaspersky a los dispositivos cliente.

Puede descargar paquetes de distribución y crear paquetes de instalación más tarde, independientemente del asistente de inicio rápido.

# Paso 8. Configurar Kaspersky Security Network

Especifique la configuración para transmitir la información sobre operaciones Kaspersky Security Center a la base de conocimientos de Kaspersky Security Network.




Configurar Kaspersky Security Network

Seleccione una de las siguientes opciones:

- **Acepto utilizar Kaspersky Security Network**

  Kaspersky Security Center y las aplicaciones administradas instaladas en dispositivos cliente transferirán automáticamente su información de operación a Kaspersky Security Network. Participar en Kaspersky Security Network permite que las bases de datos con información sobre virus y otros riesgos se actualicen más rápidamente, lo cual se traduce en una mayor velocidad de respuesta ante amenazas a la seguridad emergentes.

- **No acepto utilizar Kaspersky Security Network**

  Kaspersky Security Center y las aplicaciones administradas no proporcionarán información a Kaspersky Security Network.

  Si selecciona esta opción, se deshabilitará el uso de Kaspersky Security Network.

Puede configurar el acceso a Kaspersky Security Network (KSN) más tarde, por separado del asistente de inicio rápido.

# Paso 9. Selección del método de activación de la aplicación

Seleccione una de las siguientes opciones de activación de Kaspersky Security Center:

- **Introducir su código de activación**

  Un *código de activación* es una secuencia única formada por 20 caracteres alfanuméricos. Se ingresa un código de activación para agregar una clave que activa Kaspersky Security Center. Recibe el código de activación en la dirección de correo electrónico que especificó después de comprar Kaspersky Security Center.

  Para activar la aplicación mediante el código de activación, necesita acceso a Internet para establecer la conexión con los servidores de activación de Kaspersky.

  Si seleccionó esta opción de activación, puede activar la opción **Distribuir la clave de licencia automáticamente a los dispositivos administrados**.

  Si esta opción está habilitada, la clave de licencia se distribuirá automáticamente a los dispositivos administrados.

  Si esta opción está desactivada, podrá distribuir la clave de licencia a los dispositivos administrados más adelante en el nodo **Licencias de Kaspersky** del árbol de la Consola de administración.

- **Especificando un archivo de clave**

  El *archivo de clave* es un archivo con la extensión .key que le proporciona Kaspersky. Los archivos de clave se usan para agregar una clave que activa la aplicación.

  Los métodos para obtener el archivo de clave se describen en la siguiente sección: Acerca del archivo de clave.

  Para activar la aplicación con un archivo de clave, no es necesario conectarse a los servidores de activación de Kaspersky.

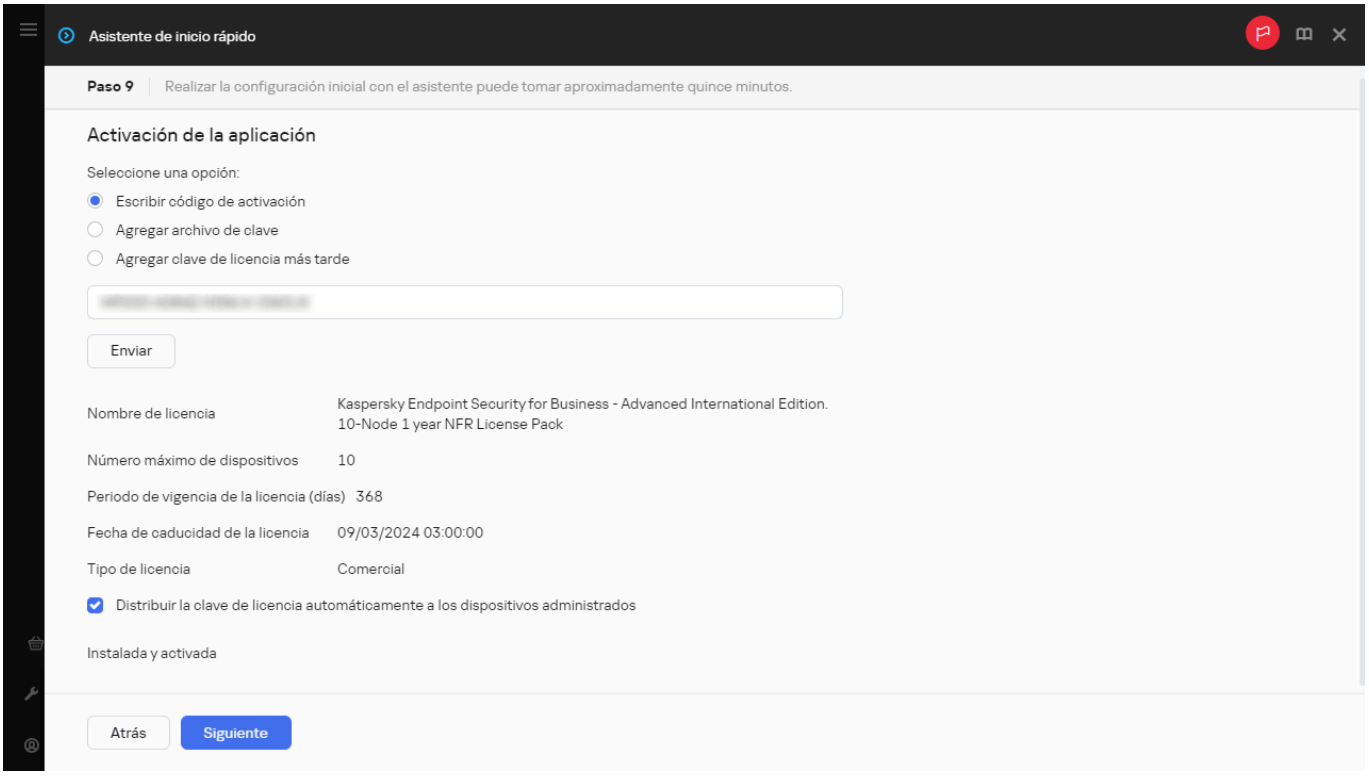
  Si seleccionó esta opción de activación, puede activar la opción **Distribuir la clave de licencia automáticamente a los dispositivos administrados**.

  Si esta opción está habilitada, la clave de licencia se distribuirá automáticamente a los dispositivos administrados.

  Si esta opción está desactivada, podrá distribuir la clave de licencia a los dispositivos administrados más adelante en el nodo **Licencias de Kaspersky** del árbol de la Consola de administración.

- **Posponiendo la activación de aplicaciones**

La aplicación funcionará con una funcionalidad básica, sin Administración de dispositivos móviles y sin Administración de vulnerabilidades y parches.



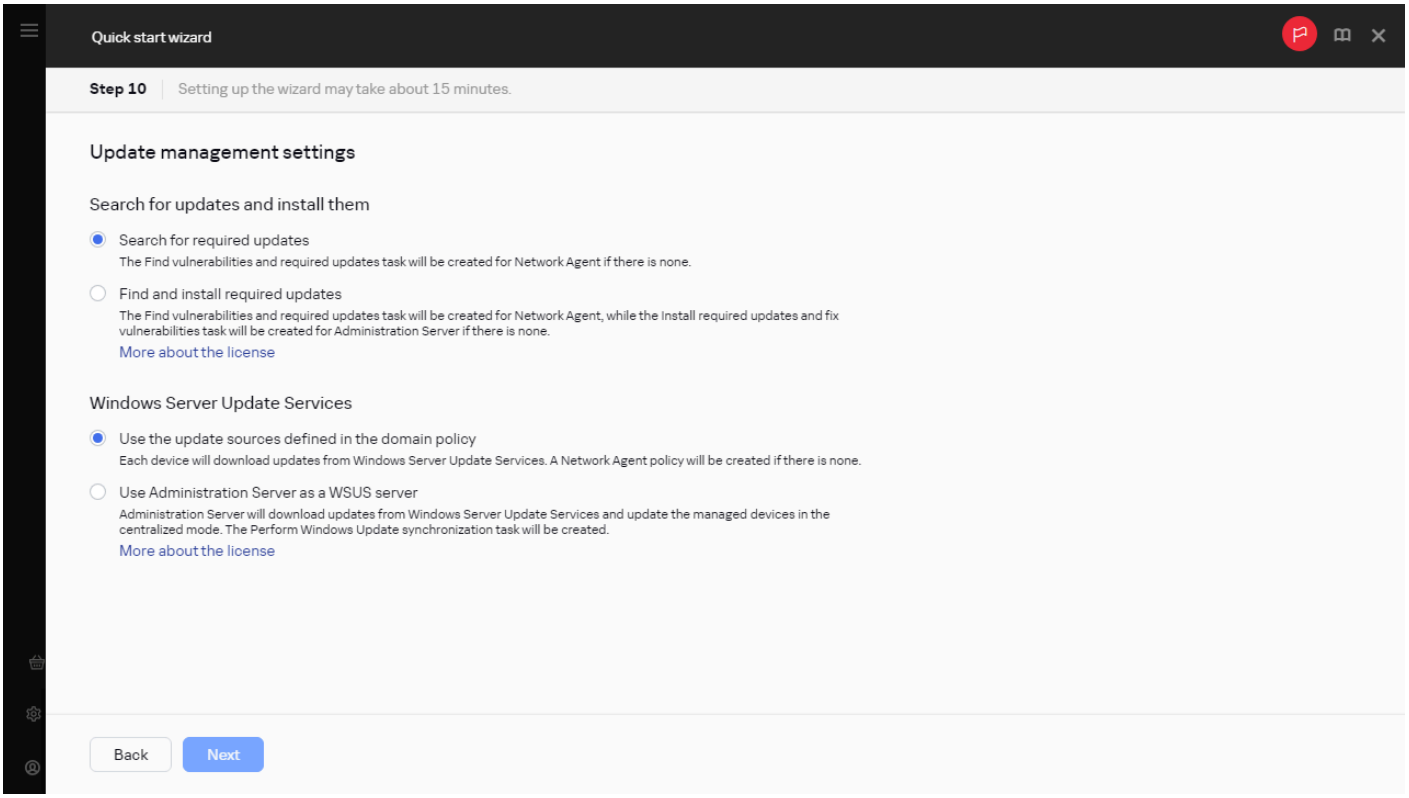

Selección del método de activación de la aplicación

Si decide posponer la activación de la aplicación, puede agregar una clave de licencia más adelante en cualquier momento **Operaciones** → **Licencias**.

Cuando trabaje con Kaspersky Security Center desplegado desde una AMI pagada o para un SKU que se facture según uso, no puede especificar un archivo de clave o ingresar un código.

# Paso 10. Especificar la configuración de administración de las actualizaciones de terceros

Este paso no se muestra si no tiene la licencia de Administración de vulnerabilidades y parches y la tarea *Buscar vulnerabilidades y actualizaciones requeridas* ya existe.




Configuración de administración de las actualizaciones de terceros

Para las actualizaciones de software de terceros, seleccione una de las siguientes opciones:

- **Buscar actualizaciones requeridas**

  La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se creará automáticamente si no existe.

  Esta opción está seleccionada de forma predeterminada.

- **Buscar e instalar actualizaciones requeridas**

  Las tareas *Buscar vulnerabilidades y actualizaciones requeridas* e *Instalar actualizaciones requeridas y reparar vulnerabilidades* se crearán automáticamente si no existen.

  Esta opción solo está disponible si se cuenta con una licencia de Administración de vulnerabilidades y parches.

Para las actualizaciones de Windows Update, seleccione una de las siguientes opciones:

- **Usar los orígenes de actualizaciones definidos en la directiva del dominio**

  Los dispositivos cliente descargarán las actualizaciones de Windows Update de conformidad con la configuración de la directiva de su dominio. La directiva del Agente de red se creará automáticamente en caso de que no exista.

- **Usar el Servidor de administración como servidor WSUS**

  Los dispositivos cliente descargarán las actualizaciones de Windows Update del Servidor de administración. La tarea *Sincronización con Windows Update* y la directiva del Agente de red se crean automáticamente si no existen.

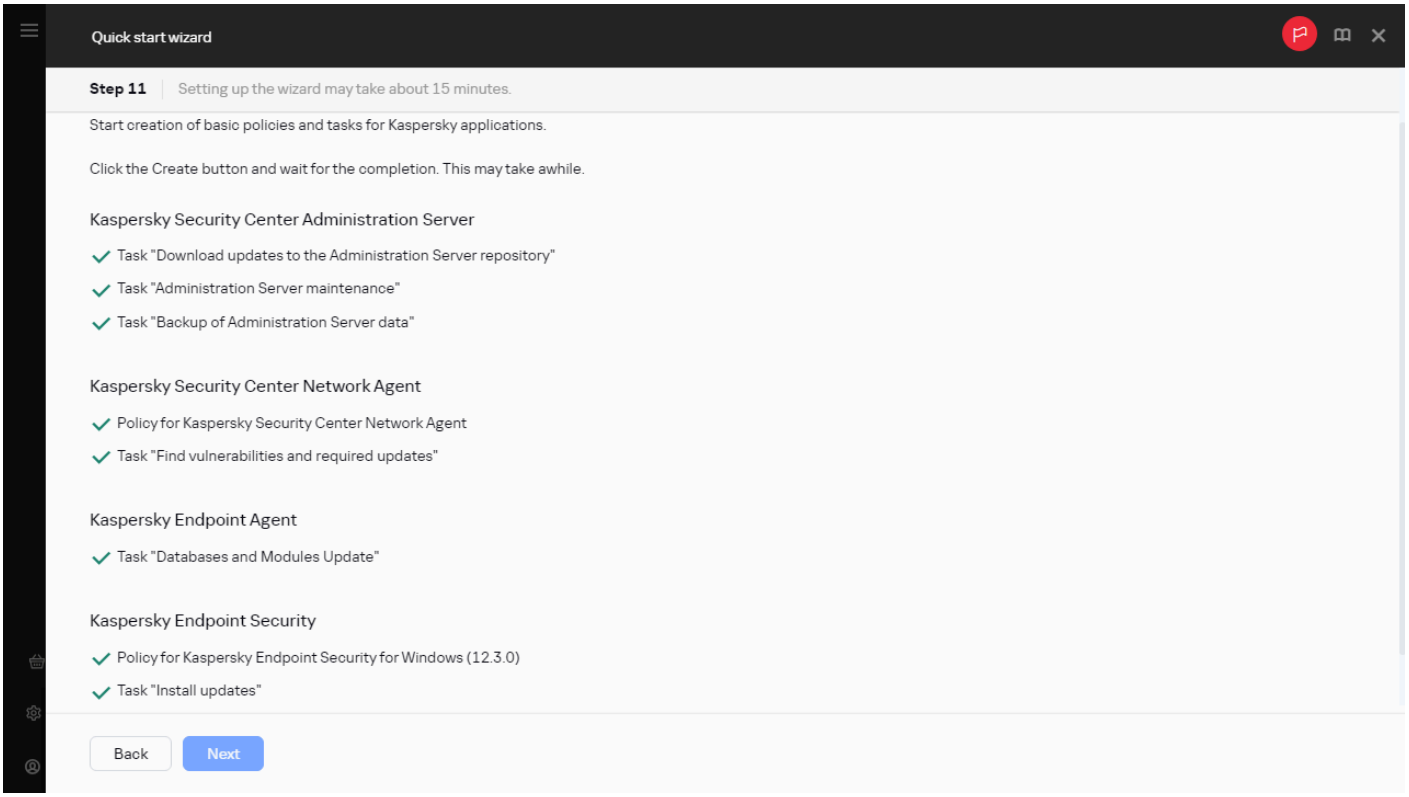
  Esta opción solo está disponible si se cuenta con una licencia de Administración de vulnerabilidades y parches.

Puede crear las tareas *Buscar vulnerabilidades y actualizaciones necesarias* e *Instalar actualizaciones necesarias y corregir vulnerabilidades* por separado desde el asistente de inicio rápido. Para usar el Servidor de administración como servidor de WSUS, debe crear la tarea *Sincronización con Windows Update* y, a continuación, seleccionar la opción **Usar el Servidor de administración como servidor WSUS** en la directiva del Agente de red.

## Paso 11. Creación de una configuración básica de protección de la red

Puede ver la lista de directivas y tareas creadas.

Espere a que terminen de crearse las tareas y directivas antes de avanzar al siguiente paso del asistente.

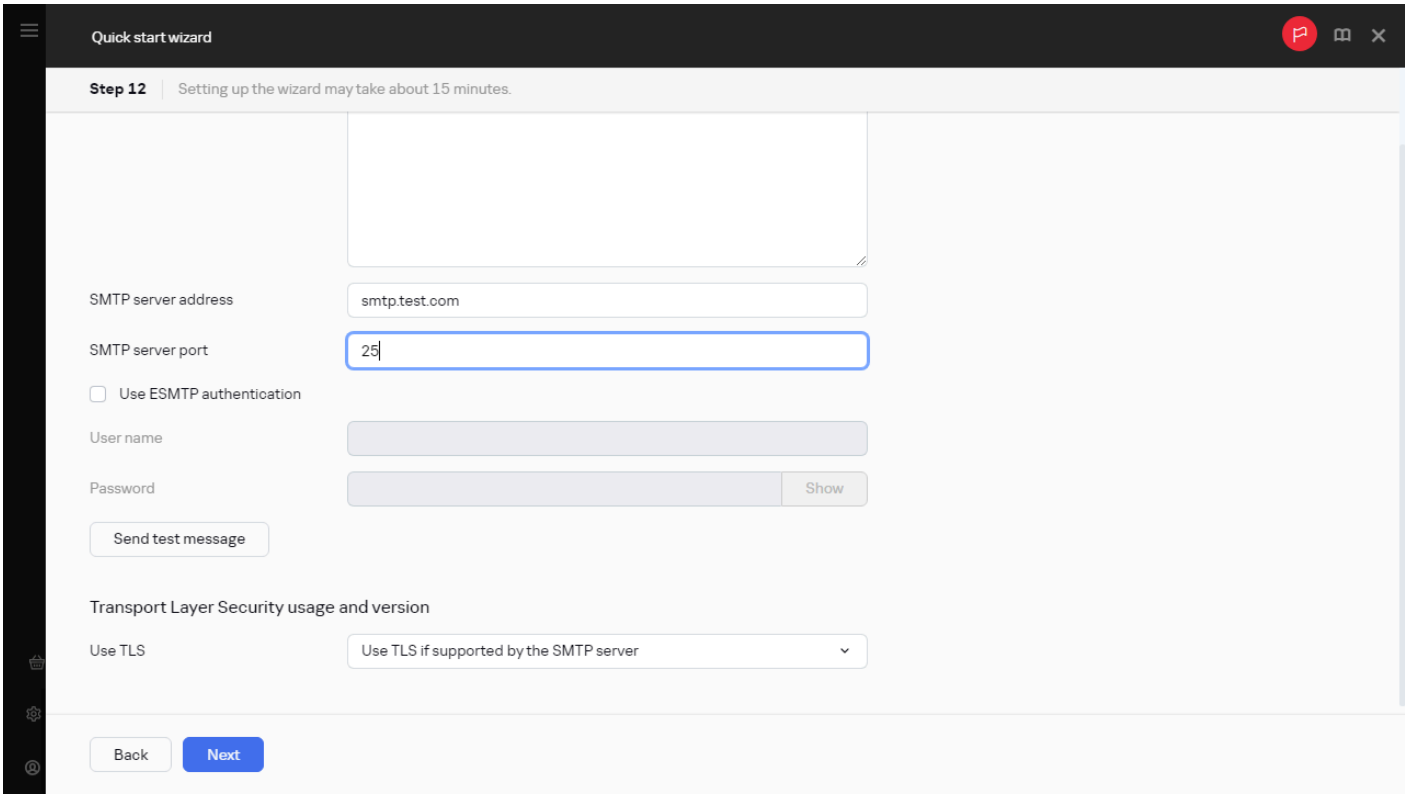



Creación de una configuración básica de protección de la red

Puede crear las tareas y directivas requeridas más tarde, sin usar el asistente de inicio rápido.

# Paso 12. Configuración de notificaciones por correo electrónico

Configure la entrega de notificaciones sobre eventos registrados durante el funcionamiento de aplicaciones Kaspersky en los dispositivos cliente. Estos parámetros servirán de configuración predeterminada de las directivas de la aplicación.




Configuración de notificaciones por correo electrónico

Para configurar la entrega de notificaciones sobre eventos que ocurren en Aplicaciones de Kaspersky, use la configuración siguiente:

- **Direcciones de los destinatarios**

  Las direcciones de correo electrónico de usuarios a quien la aplicación enviará notificaciones. Puede ingresar una o más direcciones; si ingresa más de una dirección, sepárelas con un punto y coma.

- **Dirección del servidor SMTP**

  La dirección o direcciones de los servidores de correo de su organización.

  Si ingresa más de una dirección, sepárelas con un punto y coma. Puede utilizar los siguientes parámetros:

  - Dirección IPv4 o IPv6
  - Nombre de la red de Windows (nombre NetBIOS) del dispositivo
  - Nombre DNS del servidor SMTP

- Puerto del servidor SMTP

  Número del puerto de comunicación del servidor SMTP. Si utiliza varios servidores SMTP, la conexión con ellos se establecerá a través del puerto de comunicación especificado. El número de puerto predeterminado es 25.

- Utilizar autenticación ESMTP

  Habilita la compatibilidad con la autenticación ESMTP. Cuando la casilla está seleccionada, en los campos **Nombre de usuario** y **Contraseña**, puede especificar la configuración de la autorización de ESMTP. Esta casilla no está marcada de manera predeterminada.

- Usar TLS

Puede especificar la configuración de TLS para la conexión con un servidor SMTP:

- **No usar TLS**

  Puede seleccionar esta opción si desea deshabilitar el cifrado de mensajes de correo electrónico.

- **Usar TLS si es compatible con el servidor SMTP**

  Puede seleccionar esta opción si desea usar una conexión TLS con un servidor SMTP. Si el servidor SMTP no es compatible con TLS, el Servidor de administración se conecta con el servidor SMTP sin usar TLS.

- **Usar siempre TLS, comprobar la validez del certificado del servidor**

  Puede seleccionar esta opción si desea usar la configuración de autenticación de TLS. Si el servidor SMTP no es compatible con TLS, el Servidor de administración no puede conectarse al servidor SMTP.

  > Le recomendamos que use esta opción para una mejor protección de la conexión con un servidor SMTP. Si selecciona esta opción, puede establecer la configuración de autenticación para una conexión TLS.

  Si selecciona el valor **Usar siempre TLS, comprobar la validez del certificado del servidor**, puede especificar un certificado para la autenticación del servidor SMTP y elegir si desea habilitar la comunicación a través de cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. También puede especificar un certificado para la autenticación de un cliente en el servidor SMTP.

Puede especificar certificados para una conexión TLS al hacer clic en el enlace **Especificar certificados**:

- Busque un archivo de certificados del servidor SMTP:

  Puede recibir un archivo con la lista de certificados de una autoridad de certificación confiable y cargar el archivo al Servidor de administración. Kaspersky Security Center verifica si el certificado de un servidor SMTP también está firmado por una autoridad de certificación confiable. Si el certificado de un servidor SMTP no se recibe de una autoridad de certificación confiable, Kaspersky Security Center no podrá conectarse al servidor SMTP.

- Busque un archivo de certificados cliente:

  Puede utilizar un certificado recibido de cualquier fuente (por ejemplo, de una entidad de certificación de confianza). Deberá especificar el certificado y su clave privada. Puede usar, para ello, alguno de los siguientes tipos de certificado:

  - Certificado X-509:

    Debe especificar un archivo con el certificado y un archivo con la clave privada. Estos dos archivos no dependen el uno del otro y el orden en que se los carga no es importante. Cuando se cargan ambos archivos, debe especificar la contraseña para decodificar la clave privada. Si la clave privada no está codificada, puede dejar la contraseña en blanco.

  - Contenedor pkcs12:

    Debe cargar un solo archivo que contenga el certificado y la clave privada. Cuando se carga el archivo, debe especificar la contraseña para decodificar la clave privada. Si la clave privada no está codificada, puede dejar la contraseña en blanco.

Puede probar la configuración de la notificación por correo electrónico nueva haciendo clic en el botón **Enviar mensaje de prueba**.

Puede configurar notificaciones de eventos más tarde, sin usar el asistente de inicio rápido.

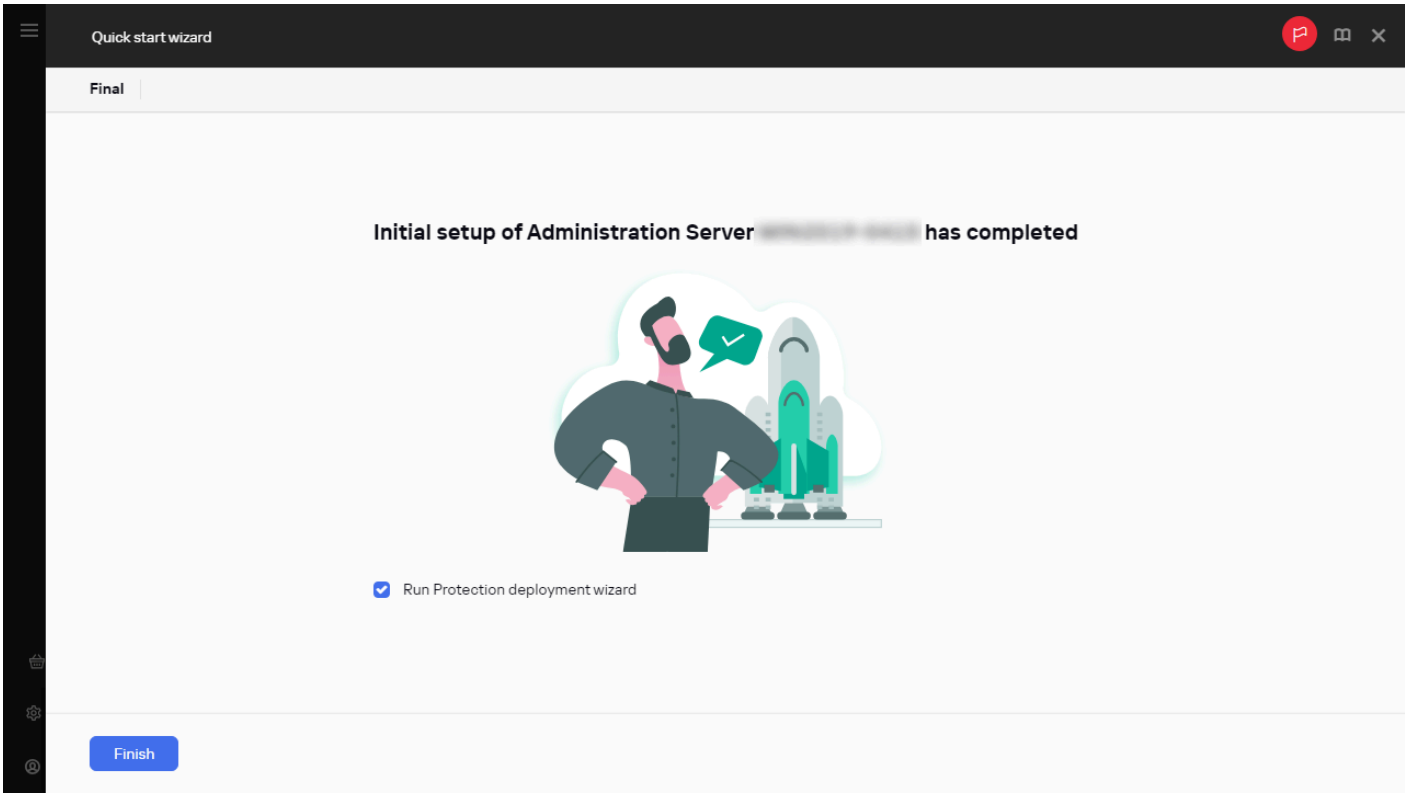
## Paso 13. Realizar un sondeo de red

El Servidor de administración realiza un sondeo inicial. Durante el sondeo, se muestra una barra de progreso. Cuando finaliza el sondeo, el vínculo **Ver dispositivos detectados** está disponible. Puede hacer clic en este enlace para ver los dispositivos de red detectados por el Servidor de administración. Para volver al Asistente de inicio rápido, presione la tecla **Escape**.

Puede sondear su red más tarde, independientemente del asistente de inicio rápido. Utilice Kaspersky Security Center Web Console para configurar el sondeo de un controlador de dominio , dominios de Windows , rangos de IP y redes IPv6 .

## Paso 14. Cierre del asistente de inicio rápido

En la página de finalización del Asistente de inicio rápido, active la casilla **Ejecutar el Asistente de despliegue de la protección** si desea iniciar la instalación automática de las aplicaciones antivirus o del Agente de red en los dispositivos de la red.




Paso final del Asistente de inicio rápido

Para cerrar el asistente, haga clic en el botón **Finalizar**.

# Conexión de dispositivos fuera de la oficina

En esta sección se explica cómo conectar dispositivos fuera de la oficina (es decir, dispositivos administrados que se encuentran fuera de la red principal) al Servidor de administración.

# Escenario: conexión de dispositivos fuera de la oficina mediante una puerta de enlace de conexión

Este escenario describe cómo conectar dispositivos administrados que se encuentran fuera de la red principal al Servidor de administración.

## Requisitos previos

El escenario tiene los siguientes requisitos previos:

- Existe una zona desmilitarizada (DMZ) en la red de su organización.
- El Servidor de administración de Kaspersky Security Center se despliega en la red corporativa.

## Etapas

Este escenario se divide en etapas:

1. **Seleccionar un dispositivo cliente en la DMZ**

   El dispositivo actuará como puerta de enlace de conexión. El dispositivo debe reunir los requisitos para puertas de enlace de conexión.

2. **Instalar el Agente de red en el rol de puerta de enlace de conexión**

   Recomendamos instalar el Agente de red en forma local en el dispositivo elegido.

   De forma predeterminada, el archivo de instalación se encuentra en \\<nombre del servidor>\KLSHARE\PkgInst\NetAgent_<número de versión>.

   En la ventana **Puerta de enlace de conexión** del Asistente de instalación del Agente de red, seleccione **Usar el Agente de red como una puerta de enlace de conexión en la DMZ**. Este modo activa simultáneamente la función de puerta de enlace de conexión y le indica al Agente de red que espere las conexiones del Servidor de administración en lugar de establecer conexiones con el Servidor de administración.

   De forma alternativa, puede instalar el Agente de red en un dispositivo Linux y configurar el Agente de red para que funcione como puerta de enlace de conexión, pero ponga atención a la lista de limitaciones del Agente de red que se ejecuta en los dispositivos Linux.

3. **Permitir las conexiones a la puerta de enlace en los distintos firewalls**

   Para asegurarse de que el Servidor de administración pueda realmente conectarse a la puerta de enlace de conexión en la DMZ, permita conexiones al puerto TCP 13000 en todos los firewalls entre el Servidor de administración y la puerta de enlace de conexión.

   Si la puerta de enlace de conexión no tiene una dirección IP real en Internet, sino que se encuentra detrás de la traducción de direcciones de red (NAT), configure una regla para reenviar las conexiones a través de la NAT.

4. **Crear un grupo de administración para dispositivos externos**

   Cree un nuevo grupo dentro del grupo **Dispositivos administrados**. El nuevo grupo albergará los dispositivos externos administrados.

5. **Conectar la puerta de enlace de conexión al Servidor de administración**

La puerta de enlace de conexión que configuró está esperando una conexión del Servidor de administración. El Servidor de administración, sin embargo, no incluye el dispositivo con la puerta de enlace de conexión entre los dispositivos administrados. Esto se debe a que la puerta de enlace no ha intentado conectarse con el Servidor de administración. El problema puede resolverse con un procedimiento especial, que obliga al Servidor de administración a conectarse con la puerta de enlace de conexión.

Haga lo siguiente:

1. Agregue la puerta de enlace de conexión como punto de distribución.
2. Mueva la puerta de enlace de conexión del grupo **Dispositivos no asignados** al grupo que creó para los dispositivos externos.

La puerta de enlace de conexión está conectada y configurada.

6. **Conectar dispositivos de escritorio externos al Servidor de administración**

   Por lo general, los dispositivos de escritorio externos no se mueven dentro del perímetro. Por lo tanto, debe configurarlas para que se conecten al Servidor de administración a través de la puerta de enlace durante la instalación del Agente de red.

7. **Configurar el mecanismo de actualización para los dispositivos de escritorio externos**

   Si las actualizaciones de las aplicaciones de seguridad están configuradas para descargarse del Servidor de administración, los dispositivos externos descargan las actualizaciones a través de la puerta de enlace de conexión. Esto conlleva dos desventajas:

   - El tráfico de Internet generado ocupa ancho de banda innecesariamente.
   - Esta no es necesariamente la forma más rápida de obtener actualizaciones. Muy probablemente, lo más rápido y económico sea que los dispositivos externos obtengan las actualizaciones de los servidores de actualizaciones de Kaspersky.

   Haga lo siguiente:

   1. Mueva todos los dispositivos externos al grupo de administración independiente que creó anteriormente.
   2. Asegúrese de que el grupo de dispositivos externos quede excluido de la tarea de actualización.
   3. Cree una tarea de actualización separada para el grupo con dispositivos externos.

8. **Conectar las computadoras portátiles de quienes viajan al Servidor de administración**

   Las computadoras portátiles de quienes viajan a veces están dentro de la red y, en otras ocasiones, afuera. Para una administración eficaz, debe conectarlas al Servidor de administración de forma diferente según su ubicación. Para un uso eficiente del tráfico, también necesitan recibir actualizaciones de diferentes fuentes según su ubicación.

   Necesita configurar reglas para usuarios fuera de la oficina: perfiles de conexión y descripciones de ubicación de red. Cada regla define la instancia del Servidor de administración al que deben conectarse las computadoras portátiles que viajan, según su ubicación y la instancia del Servidor de administración desde el cual deben recibir actualizaciones.

## Escenario: Conectar dispositivos fuera de la oficina mediante un Servidor de administración secundario en la DMZ

Si desea conectar dispositivos administrados que estén fuera de la red principal al Servidor de Administración, puede hacerlo mediante un Servidor de Administración secundario que se encuentre en la zona desmilitarizada (DMZ).

### Requisitos previos

Antes de comenzar, compruebe que hizo lo siguiente:

- Existe una zona desmilitarizada (DMZ) en la red de su organización.
- El Servidor de administración de Kaspersky Security Center queda desplegado en la red corporativa.

### Etapas

Este escenario se divide en etapas:

1. **Seleccionar un dispositivo cliente en la DMZ**

   En la DMZ, seleccione un dispositivo cliente que se utilizará como puerta de enlace de conexión.

2. **Instalar el Servidor de administración de Kaspersky Security Center**

   Para instalar el Servidor de administración de Kaspersky Security Center en este dispositivo local.

3. **Crear una jerarquía de Servidores de administración**

   Si coloca un Servidor de administración secundario en la DMZ, éste debe recibir una conexión proveniente del Servidor de Administración primario. Puede agregar un nuevo Servidor de administración como secundario para que el Servidor de administración principal se conecte al Servidor de administración secundario a través del puerto 13000. Al combinar dos Servidores de administración en una jerarquía, asegúrese de que el puerto 13299 esté accesible en ambos Servidores de administración. Kaspersky Security Center Web Console se conecta a un Servidor de administración a través del puerto 13299.

4. **Conexión de los dispositivos fuera de la oficina con el Servidor de administración secundario**

   Puede conectar dispositivos que estén fuera de la oficina al Servidor de administración en la DMZ de la misma manera en que se conecta el Servidor de administración y los dispositivos administrados que se encuentran en la red principal. Los dispositivos administrados fuera de la oficina inician la conexión a través del puerto 13000.

## Acerca de la conexión de dispositivos fuera de la oficina

Algunos dispositivos administrados siempre se encuentran fuera de la red principal (por ejemplo, los dispositivos en las sucursales regionales de una empresa; los quioscos, los cajeros automáticos y las terminales instaladas en diversos puntos de venta; dispositivos en las oficinas domésticas de los empleados). Algunos dispositivos se mueven hacia fuera del perímetro de vez en cuando (por ejemplo, las computadoras portátiles de usuarios que visitan sucursales regionales o la oficina de un cliente).

Aún necesita monitorear y administrar la protección de los dispositivos fuera de la oficina, recibir información real sobre su estado de protección y mantener las aplicaciones de seguridad en ellos en el estado actualizado. Esto es necesario porque, por ejemplo, si un dispositivo de este tipo se ve comprometido mientras está lejos de la red principal, podría convertirse en una plataforma para propagar amenazas tan pronto como se conecte a la red principal. Para conectar dispositivos fuera de la oficina al Servidor de administración, puede utilizar los dos métodos siguientes:

- Una puerta de enlace de conexión en la zona desmilitarizada (DMZ)

  Consulte el esquema de tráfico de datos: Servidor de administración en una LAN, dispositivos administrados en Internet, puerta de enlace de conexión en uso

- Un Servidor de administración en DMZ

  Consulte el esquema de tráfico de datos: Servidor de administración en una DMZ, dispositivos administrados en Internet

## Una puerta de enlace de conexión en la DMZ

Un método recomendado para conectar al Servidor de administración dispositivos que están fuera de la oficina consiste en preparar una DMZ en la red de la organización e instalar una puerta de enlace de conexión en la DMZ. Los dispositivos externos se conectarán a la puerta de enlace de conexión, y el Servidor de administración dentro de la red iniciará la conexión con los dispositivos a través de la puerta de enlace de conexión.

En comparación con el otro método, este es más seguro por los siguientes motivos:

- No es necesario abrir el acceso al Servidor de administración desde fuera de la red.

- Una puerta de enlace de conexión comprometida no representa un riesgo elevado para la seguridad de los dispositivos de red. En realidad, una puerta de enlace de conexión no administra ningún elemento por sí misma y no establece ninguna conexión.

Además, una puerta de enlace de conexión no necesita muchos recursos de hardware.

Sin embargo, este método implica un proceso de configuración más complejo:

- Para que un dispositivo funcione como una puerta de enlace de conexión en la DMZ, debe instalar el Agente de red y conectarlo al Servidor de administración de una forma muy concreta.

- No podrá utilizar la misma dirección para conectarse al Servidor de administración en todas las situaciones. Desde fuera del perímetro, deberá emplear no solo una dirección diferente (la dirección de la puerta de enlace de conexión), sino también un modo de conexión diferente: a través de una puerta de enlace de conexión.

- También debe definir una configuración de conexión diferente para las computadoras portátiles que se encuentren en diferentes ubicaciones.

*Para agregar una puerta de enlace de conexión a una red ya configurada:*

1. Instale el Agente de red en el modo de puerta de enlace de conexión.

2. Vuelva a instalar el Agente de red en los dispositivos que desee conectar a la puerta de enlace de conexión recién agregada.

### Un Servidor de administración en la DMZ

Otro método consiste en instalar un único Servidor de administración en la DMZ.

Esta configuración es menos segura que el método anterior. En este caso, para administrar computadoras portátiles externas, el Servidor de administración debe aceptar conexiones desde cualquier dirección de Internet. Continuará administrando todos los dispositivos de la red interna, pero desde la DMZ. Por lo tanto, un Servidor comprometido podría hacer mucho daño, a pesar de la baja probabilidad de que tal evento ocurra.

El riesgo se reduce significativamente si el Servidor de administración en la DMZ no administra dispositivos en la red interna. Por ejemplo, un proveedor de servicios puede utilizar una configuración de este tipo para administrar los dispositivos de los clientes.

Es posible que desee utilizar este método en los siguientes casos:

- Si está familiarizado con la instalación y configuración del Servidor de administración y no desea realizar otro procedimiento para instalar y configurar una puerta de enlace de conexión.
- Si necesita administrar más dispositivos. La capacidad máxima que admite el Servidor de administración es de 100 000 dispositivos, mientras que una puerta de enlace de conexión puede admitir hasta 10 000 dispositivos.

Esta solución también acarrea algunas posibles dificultades:

- El Servidor de administración necesita una base de datos más y más recursos de hardware.
- La información sobre los dispositivos se almacenará en dos bases de datos no relacionadas (una para el Servidor de administración dentro de la red y otra en la DMZ), lo que complica la supervisión.
- Para administrar todos los dispositivos, el Servidor de administración debe estar asociado en una jerarquía, lo que dificulta no solo la supervisión, sino también la administración. Una instancia del Servidor de administración secundario impone limitaciones en las posibles estructuras de los grupos de administración. Debe decidir de qué manera y qué tareas y directivas distribuirá a una instancia del Servidor de administración secundario.
- Configurar dispositivos externos para utilizar el Servidor de administración en la DMZ de forma externa y utilizar el Servidor de administración principal de forma local no es más simple que configurarlos para utilizar una conexión condicional mediante una puerta de enlace.
- Riesgos de seguridad elevados. Si hay una instancia del Servidor de administración comprometida, es más fácil que sus computadoras portátiles administradas se vean comprometidas. Si esto sucede, los hackers solo deben esperar a que una de las computadoras portátiles vuelva a conectarse a la red corporativa para poder continuar con su ataque en la red de área local.

## Conectar dispositivos de escritorio externos al Servidor de administración

Los dispositivos de escritorio que siempre se encuentran fuera de la red principal (por ejemplo, los dispositivos en las sucursales regionales de la empresa, los cajeros automáticos y los dispositivos ubicados en los hogares de los empleados, en los puntos de venta o en las sucursales de la empresa) no se pueden conectar al Servidor de administración en forma directa. Deben hacerlo, en cambio, a través de una puerta de enlace de conexión instalada en la zona desmilitarizada (DMZ). Esta configuración se realiza al instalar el Agente de red en esos dispositivos.

*Para conectar dispositivos de escritorio externos al Servidor de administración:*

1. Cree un paquete de instalación nuevo para el Agente de red.
2. Abra las propiedades del paquete de instalación que acaba de crear y vaya a **Configuración** → **Avanzado**; luego, habilite la opción **Conectarse al Servidor de administración mediante una puerta de enlace de conexión**.

   La opción **Conectarse al Servidor de administración mediante una puerta de enlace de conexión** no es compatible con la opción **Usar el Agente de red como una puerta de enlace de conexión en la DMZ**. No puede habilitar estas dos configuraciones al mismo tiempo.

3. En el campo **Dirección de la puerta de enlace de conexión**, introduzca la dirección pública de la puerta de enlace de conexión.

   Si la puerta de enlace de conexión se encuentra detrás de la traducción de direcciones de red (NAT) y no tiene su propia dirección pública, configure una regla de puerta de enlace NAT para reenviar conexiones desde la dirección pública a la dirección interna de la puerta de enlace de conexión.

4. Cree un paquete de instalación independiente basado en el paquete de instalación creado.
5. Entregue el paquete de instalación independiente a los dispositivos de destino. Puede usar para ello una unidad extraíble u otro medio electrónico.
6. Instale el Agente de red desde el paquete independiente.

Los dispositivos de escritorio externos se conectan al Servidor de administración.

## Acerca de los perfiles de conexión para los usuarios fuera de la oficina

Los usuarios de computadoras portátiles fuera de la oficina (más adelante también llamadas "dispositivos") tal vez tengan que cambiar el método de conexión a un Servidor de administración o entre Servidores de administración, según la ubicación actual del dispositivo en la red de la empresa.

Los perfiles de conexión solo son compatibles con dispositivos que ejecutan Windows y MacOS.

### Utilización de direcciones diferentes de un Servidor de administración solo

Los dispositivos con Agente de red instalado pueden conectarse al Servidor de administración desde la red interna de la organización o desde Internet. Esta situación puede requerir que el Agente de red use direcciones diferentes para la conexión con el Servidor de administración: dirección externa del Servidor de administración para conexión a Internet y dirección interna del Servidor de administración para la conexión a la red interna.

Para ello, agregue un perfil para la conexión al Servidor de administración desde Internet en las propiedades de la directiva del Agente de red (en la sección **Configuración de la aplicación → Conectividad → Perfiles de conexión → Perfiles de conexión al Servidor de administración**). En la ventana de creación de perfil, deshabilite la opción **Usar para recibir actualizaciones solamente** y verifique que esté habilitada la opción **Sincronizar configuración de conexión con la configuración del Servidor de administración especificada en este perfil**. Si usa una puerta de enlace de conexión para acceder al Servidor de administración (por ejemplo, en una configuración de Kaspersky Security Center como la que se describe en Acceso a Internet: Agente de red como puerta de enlace de conexión en una DMZ), debe especificar la dirección de la puerta de enlace de conexión en el campo correspondiente del perfil de conexión.

### Conmutación entre Servidores de administración según la red actual

Si la organización tiene varias oficinas con Servidores de administración diferentes y algunos dispositivos con Agentes de red instalados se transfieren entre ellos, necesita un Agente de red para conectarse al Servidor de administración de la red local en la oficina donde el dispositivo se localiza actualmente.

Para este fin, en las propiedades de la directiva del Agente de red, cree perfiles para que el Agente de red se conecte al Servidor de administración de cada una de las oficinas, excepto la oficina de origen, en la que se encuentre el Servidor de administración doméstico. En los perfiles de conexión, especifique la dirección de los servidores de administración y habilite o deshabilite la opción **Usar para recibir actualizaciones solamente** según el caso:

- Habilite la opción si necesita que el Agente de red se sincronice con el Servidor de administración doméstico mientras usa el Servidor local para descargar actualizaciones únicamente.
- Deshabilite la opción si es necesario para que el Agente de red sea administrado completamente por el Servidor de administración local.

Después de esto, debe configurar las condiciones de conmutación para los perfiles recién creados: al menos una condición para cada una de las oficinas, excepto la oficina local. El propósito de cada condición consiste en la detección de elementos que son específicos para el entorno de la red de una oficina. Si una condición es verdadera, el perfil correspondiente se activa. Si ninguna de las condiciones es verdadera, el Agente de red cambia al Servidor de administración doméstico.

## Creación de un perfil de conexión para usuarios fuera de la oficina

Los perfiles para establecer conexión con un Servidor de administración solo están disponibles para dispositivos con Windows y macOS.

*Para crear un perfil para la conexión del Agente de red con el Servidor de administración para usuarios fuera de la oficina, haga lo siguiente:*

1. Si desea crear un perfil de conexión para un grupo de dispositivos administrados, abra la directiva del Agente de red correspondiente al grupo en cuestión. Para ello, realice las siguientes acciones:

   a. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.

   b. Haga clic en el vínculo de la ruta en la que se encuentre.

   c. En la ventana que se abre, seleccione el grupo de administración.

      La ruta cambiará.

   d. Agregue la directiva del Agente de red para el grupo de dispositivos administrados. Si esa directiva ya existe, haga clic en el nombre de la misma para abrir sus propiedades.

2. Si desea crear un perfil de conexión para un dispositivo administrado específico, haga lo siguiente:

   a. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.

   b. Haga clic en el nombre del dispositivo administrado.

   c. En la ventana que se abre, que contendrá las propiedades del dispositivo administrado, vaya a la pestaña **Aplicaciones**.

   d. Haga clic en el nombre de la directiva del Agente de red a la que solo aplique el dispositivo administrado seleccionado.

3. En la ventana de propiedades que se abre, vaya a **Configuración de la aplicación** → **Conectividad** → **Perfiles de conexión.**

4. En la sección **Perfiles de conexión al Servidor de administración** haga clic en el botón **Agregar**.

   De forma predeterminada, la lista de perfiles de conexión contiene los perfiles <Modo sin conexión> y <Servidor de administración doméstico>. Los perfiles no pueden ser modificados o eliminados.

   El perfil <Modo sin conexión> no especifica ningún Servidor para la conexión. Por lo tanto, el Agente de red, cuando se cambia a ese perfil, no intenta conectarse a ningún Servidor de administración mientras las aplicaciones instaladas en los dispositivos cliente se ejecutan bajo directivas fuera de la oficina. El perfil <Modo sin conexión> puede ser utilizado si los dispositivos están desconectados de la red.

   El perfil <Servidor de administración doméstico> se utiliza para establecer conexión con el Servidor de administración seleccionado durante la instalación del Agente de red. El perfil <Servidor de administración doméstico> se aplica cuando un dispositivo se conecta de nuevo al Servidor de administración doméstico después de haberse ejecutado en una red externa durante algún tiempo.

5. En la ventana **Perfil de configuración** que se abre, configure el perfil de conexión:

   - **Nombre del perfil**

     En el campo de entrada, puede ver o modificar el nombre del perfil de conexión.

   - **Dirección del Servidor de administración**

     La dirección del Servidor de administración a la que debe conectarse el dispositivo cliente al activarse el perfil.

   - **Número de puerto**

     Número de puerto que se utilizará para la conexión.

   - **Puerto SSL**

     Número de puerto para la conexión si se utiliza el protocolo SSL.

   - **Usar conexión SSL**

     Si se habilita esta opción, la conexión se establece a través un puerto seguro mediante el protocolo SSL.

     Esta opción está activada de forma predeterminada. Recomendamos no deshabilitar esta opción; de lo contrario, la conexión quedará desprotegida.

   - Seleccione la opción **Usar servidor proxy** si desea usar un servidor proxy al conectarse a Internet. Si selecciona esta opción, se habilitarán campos para que configure los ajustes pertinentes. Deberá introducir los siguientes valores de conexión del servidor proxy:

     - **Dirección**

       Dirección del servidor proxy usado para conectar Kaspersky Security Center con Internet.

     - **Número de puerto**

Número del puerto a través del cual se establecerá la conexión proxy de Kaspersky Security Center.

- **Autenticación del servidor proxy**

  Si se selecciona esta casilla, en los campos de entrada se podrán especificar las credenciales para la autenticación del servidor proxy.

- **Nombre de usuario**

  Cuenta de usuario con la que se establece la conexión al servidor proxy (este campo está disponible si se selecciona la casilla **Autenticación del servidor proxy**).

- **Contraseña**

  Contraseña que especifica el usuario con cuya cuenta se establece la conexión al servidor proxy (este campo está disponible si se selecciona la casilla **Autenticación del servidor proxy**).

  Para ver la contraseña indicada, mantenga presionado el botón **Mostrar** durante la cantidad de tiempo que sea necesario.

- **Dirección de la puerta de enlace de conexión**

  La dirección de la puerta de enlace a través de la cual los dispositivos cliente se conectan al Servidor de administración.

- **Habilitar el modo de fuera de la oficina cuando el Servidor de administración no esté disponible**

  Marque esta casilla para permitir que las aplicaciones instaladas en un dispositivo cliente usen perfiles de directiva para dispositivos en modo fuera de la oficina, así como directivas para fuera de la oficina, en cualquier intento de conexión si el Servidor de administración no está disponible. Si no hay una directiva fuera de la oficina definida para la aplicación, se utilizará la directiva activa.

  Si se deshabilita esta opción, las aplicaciones utilizarán directivas activas.

  Esta casilla no está marcada de manera predeterminada.

- **Usar para recibir actualizaciones solamente**

  Si se habilita esta opción, el perfil se utilizará solamente para que las aplicaciones instaladas en el dispositivo cliente descarguen actualizaciones. Para otras operaciones, la conexión al Servidor de administración será establecida con los parámetros de conexión iniciales definidos durante la instalación del Agente de red.

  Esta opción está activada de forma predeterminada.

- **Sincronizar configuración de conexión con la configuración del Servidor de administración especificada en este perfil**

Si se habilita esta opción, el Agente de red se conectará al Servidor de administración usando la configuración especificada en las propiedades del perfil.

Si se deshabilita esta opción, el Agente de red se conectará al Servidor de administración usando la configuración original especificada durante la instalación.

Esta opción estará disponible si la opción **Usar para recibir actualizaciones solamente** se encuentra deshabilitada.

Esta opción está deshabilitada de forma predeterminada.

Se creará un perfil para la conexión del Agente de red con el Servidor de administración para usuarios fuera de la oficina. Cuando el Agente de red se conecte al Servidor de administración con el nuevo perfil, las aplicaciones instaladas en el dispositivo cliente quedarán sujetas a directivas para dispositivos en modo fuera de la oficina o directivas para fuera de la oficina.

## Acerca de cambiar el Agente de red a otros Servidores de administración

Kaspersky Security Center ofrece la opción de cambiar el Agente de red de un dispositivo cliente a otros Servidores de administración si se han modificado las siguientes opciones de configuración de red:

- **Condición para la dirección del servidor DHCP**: La dirección IP del servidor del Protocolo de configuración dinámica de host (DHCP) de la red ha cambiado.
- **Condición para dirección predeterminada de la puerta de enlace de conexión**: la dirección de la puerta de enlace principal de la red ha cambiado.
- **Condición para dominio DNS**: cambió el sufijo DNS de la subred.
- **Condición para la dirección del servidor DNS**: cambió la dirección IP del servidor DNS de la red.
- **Condición para la dirección del servidor WINS**: cambió la dirección IP del servidor WINS de la red. Este parámetro solo está disponible para dispositivos con Windows.
- **Condición para la resolución de nombres**: el nombre DNS o NetBIOS del dispositivo cliente cambió.
- **Condición para subred**: la máscara y la dirección de subred cambiaron.
- **Condición para la accesibilidad del dominio de Windows**: el estado del dominio de Windows al cual está conectado el dispositivo cliente cambió. Este parámetro solo está disponible para dispositivos con Windows.
- **Condición para la accesibilidad de la dirección de conexión SSL**: el dispositivo cliente puede o no puede (según la opción que seleccione) establecer una conexión SSL con un Servidor específico (nombre: puerto). Para la conexión, use un servidor dedicado con software capaz de soportar una carga elevada y solicitudes frecuentes procedentes del Agente de administración. No especifique el puerto del Servidor de administración. Para cada servidor, además puede especificar un certificado SSL. En este caso, el Agente de red verifica el certificado del servidor además de verificar la capacidad de una conexión SSL. Si el certificado no coincide, la conexión genera un error.

Esta función solo es compatible con agentes de red instalados en dispositivos con Windows o macOS.

La configuración inicial de la conexión del Agente de red al Servidor de administración se define durante la instalación del Agente de red. Posteriormente, si se han creado reglas para cambiar el Agente de red a otros Servidores de administración, el Agente de red responde a los cambios en la configuración de red del siguiente modo:

- Si la configuración de la red cumple con una de las reglas creadas, el Agente de red se conecta con el Servidor de administración especificado en esta regla. Las aplicaciones instaladas en dispositivos cliente cambian a directivas fuera de la oficina siempre que este comportamiento esté habilitado por una regla.
- Si no se aplica ninguna de las reglas, el Agente de red revertirá a la configuración predeterminada de la conexión con el Servidor de administración especificado durante la instalación. Las aplicaciones instaladas en dispositivos cliente vuelven a las directivas activas.
- Si el Servidor de administración no es accesible, el Agente de red utilizará las directivas fuera de la oficina.

Para que el Agente de red pase a utilizar una directiva fuera de la oficina, es necesario que la opción **Habilitar el modo de fuera de la oficina cuando el Servidor de administración no esté disponible** esté habilitada en la directiva del Agente de red.

La configuración de la conexión del Agente de red al Servidor de administración se guarda en un perfil de conexión. En el perfil de conexión puede crear reglas para cambiar dispositivos cliente a directivas fuera de la oficina además de configurar el perfil para que pueda utilizarse solo para descargar actualizaciones.

## Creación de una regla de conmutación del Agente de red por ubicación de red

Para que el Agente de red pueda cambiar de Servidor de administración según la ubicación de red del dispositivo, el dispositivo debe utilizar Windows o macOS.

*Para crear una regla para que el Agente de red cambie de un Servidor de administración a otro si la configuración de la red cambia:*

1. Si desea crear una regla para un grupo de dispositivos administrados, abra la directiva del Agente de red correspondiente al grupo en cuestión. Para ello, realice las siguientes acciones:

   a. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.

   b. Haga clic en el vínculo de la ruta en la que se encuentre.

   c. En la ventana que se abre, seleccione el grupo de administración.

   La ruta cambiará.

   d. Agregue la directiva del Agente de red para el grupo de dispositivos administrados. Si esa directiva ya existe, haga clic en el nombre de la misma para abrir sus propiedades.

2. Si desea crear una regla para un dispositivo administrado específico, haga lo siguiente:

   a. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.

   b. Haga clic en el nombre del dispositivo administrado.

   c. En la ventana que se abre, que contendrá las propiedades del dispositivo administrado, vaya a la pestaña **Aplicaciones**.

   d. Haga clic en el nombre de la directiva del Agente de red a la que solo aplique el dispositivo administrado seleccionado.

3. En la ventana de propiedades que se abre, vaya a **Configuración de la aplicación** → **Conectividad** → **Perfiles de conexión.**

4. En la sección **Configuración de ubicación de red**, haga clic en el botón **Agregar**.

5. En la ventana de propiedades que se abre, configure la descripción de la ubicación de red y la regla de conmutación. Especifique los siguientes parámetros de la descripción de la ubicación de red:

   - **Descripción**

     El nombre de una descripción de ubicación de red no puede ser más largo que 255 caracteres, ni contener símbolos especiales, por ejemplo ("*<>?\/:|).

   - **Usar perfil de conexión**

     En la lista desplegable, puede especificar el perfil de conexión que utiliza el Agente de red para conectarse al Servidor de administración. Este perfil se utilizará cuando las condiciones de la descripción de la ubicación de red se cumplan. El perfil de conexión contiene la configuración para conectar al Agente de red al Servidor de administración; también define cuándo los dispositivos cliente deben cambiar a las directivas fuera de la oficina. El perfil se utiliza solamente para descargar actualizaciones.

   - **Descripción habilitada**

     Marque esta casilla para habilitar el uso de la nueva descripción de ubicación de red.

6. Seleccione las condiciones para la regla de conmutación del Agente de red:

   - **Condición para la dirección del servidor DHCP**: La dirección IP del servidor del Protocolo de configuración dinámica de host (DHCP) de la red ha cambiado.
   - **Condición para dirección predeterminada de la puerta de enlace de conexión**: la dirección de la puerta de enlace principal de la red ha cambiado.
   - **Condición para dominio DNS**: cambió el sufijo DNS de la subred.
   - **Condición para la dirección del servidor DNS**: cambió la dirección IP del servidor DNS de la red.
   - **Condición para la dirección del servidor WINS**: cambió la dirección IP del servidor WINS de la red. Este parámetro solo está disponible para dispositivos con Windows.
   - **Condición para la resolución de nombres**: el nombre DNS o NetBIOS del dispositivo cliente cambió.
   - **Condición para subred**: la máscara y la dirección de subred cambiaron.
   - **Condición para la accesibilidad del dominio de Windows**: el estado del dominio de Windows al cual está conectado el dispositivo cliente cambió. Este parámetro solo está disponible para dispositivos con Windows.
   - **Condición para la accesibilidad de la dirección de conexión SSL**: el dispositivo cliente puede o no puede (según la opción que seleccione) establecer una conexión SSL con un Servidor específico (nombre: puerto). Para cada servidor, además puede especificar un certificado SSL. En este caso, el Agente de red verifica el certificado del Servidor además de verificar la capacidad de una conexión SSL. Si el certificado no coincide, la conexión genera un error.

   Las condiciones de una regla se combinan con el operador lógico AND. Para desencadenar una regla que cambia por la descripción de la ubicación de la red, todas las reglas de conmutación de las condiciones se deben cumplir.

7. En la sección de condiciones, indique cuándo deberá cambiar de Servidor de administración el Agente de red. Para ello, haga clic en el botón **Agregar** y defina el valor de la condición.

   Tenga en cuenta que la opción **Coincide al menos con un valor de la lista** está habilitada por defecto. Puede deshabilitar esta opción para exigir que se cumplan todos los valores especificados para la condición.

8. Guarde sus cambios.

Se creará una nueva regla de conmutación según la descripción de la ubicación de red; cada vez que las condiciones se cumplan, el Agente de red utilizará el perfil de conexión especificado en la regla para conectarse al Servidor de administración.

# Asistente de despliegue de la protección

Puede usar el Asistente de despliegue de la protección para instalar aplicaciones de Kaspersky. El Asistente de despliegue de la protección permite la instalación remota de aplicaciones mediante paquetes de instalación creados previamente o directamente desde un paquete de distribución.

El Asistente de despliegue de la protección realiza las siguientes acciones:

- Descarga un paquete de instalación para instalar la aplicación deseada (si el paquete no se creó de antemano). El paquete de instalación se ubica en **Descubrimiento y despliegue → Despliegue y asignación → Paquetes de instalación**. El paquete puede usarse para instalar la aplicación en otro momento.

- Crea y ejecuta una tarea de instalación remota para dispositivos específicos o para un grupo de administración. La nueva tarea de instalación remota se agrega a la sección **Tareas**. Podrá iniciar la tarea manualmente cuando lo desee. El tipo de tarea es **Instalar aplicación de forma remota**.

Si desea instalar el Agente de red en dispositivos con el sistema operativo SUSE Linux Enterprise Server 15, primero, instale el paquete insserv-compat para configurar el Agente de red.

# Paso 1. Iniciar el Asistente de despliegue de la protección

*Para iniciar manualmente el Asistente de despliegue de la protección,*

En el menú principal, vaya a **Descubrimiento y despliegue → Despliegue y asignación → Asistente de despliegue de la protección**.

Se abre el Asistente de despliegue de la protección. Avance por el asistente utilizando el botón **Siguiente**.

# Paso 2. Seleccionar el paquete de instalación

Seleccione el paquete de instalación de la aplicación que desee instalar.

Si el paquete de instalación de la aplicación requerida no está en la lista, haga clic en el botón **Agregar** y luego seleccione la aplicación en la lista.

# Paso 3. Selección de un método para la distribución del archivo de clave o código de activación

Seleccione un método para la distribución del archivo de clave o el código de activación:

- **No agregar una clave de licencia al paquete de instalación**

  La clave se distribuirá automáticamente a todos los dispositivos con los que sea compatible si se cumplen las siguientes condiciones:

  - Si se habilitó la distribución automática en las propiedades de la clave.
  - Si se creó la tarea **Agregar clave**.

- **Agregar una clave de licencia al paquete de instalación**

  La clave se distribuirá a los dispositivos con el paquete de instalación.

  No le recomendamos distribuir la clave con este método, ya que los derechos Acceso de lectura compartidos están activados para el repositorio de paquetes de instalación.

Si el paquete de instalación ya contiene un archivo de clave o un código de activación, la ventana solo mostrará los información de la clave de licencia.

# Paso 4. Seleccionar la versión del Agente de red

Si el paquete de instalación que seleccionó no fue el del Agente de red, también deberá instalar el Agente de red, que conecta la aplicación con el Servidor de administración de Kaspersky Security Center.

Seleccione la última versión del Agente de red.

# Paso 5. Seleccionar los dispositivos

Especifique una lista de dispositivos en los que se instalará la aplicación:

- **Instalar en dispositivos administrados**

  Si selecciona esta opción, la tarea de instalación remota se creará para un grupo de dispositivos.

- **Seleccionar los dispositivos para la instalación**

  La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

  Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

# Paso 6. Configurar la tarea de instalación remota

En la página **Configuración de la tarea de instalación remota**, especifique la configuración para la instalación remota de la aplicación.

En el grupo de configuraciones **Forzar la descarga del paquete de instalación**, puede especificar cómo se distribuyen a los dispositivos cliente los archivos que se requieren para la instalación de una aplicación:

- **Con el Agente de red**

  Si habilita esta opción, los paquetes de instalación se transferirán a los dispositivos cliente a través del Agente de red instalado en esos dispositivos.

  Si no habilita esta opción, los paquetes de instalación se distribuirán utilizando las herramientas provistas por el sistema operativo de los dispositivos cliente.

  Recomendamos habilitar esta opción si la tarea está asignada a dispositivos que tienen instalado el Agente de red.

  Esta opción está habilitada de manera predeterminada.

- **Con los recursos del sistema operativo a través de los puntos de distribución**

  Si habilita esta opción, los paquetes de instalación se transferirán a los dispositivos cliente mediante las herramientas del sistema operativo a través de los puntos de distribución. Puede seleccionar esta opción si existe al menos un punto de distribución en la red.

  Si habilitó la opción **Con el Agente de red**, las herramientas del sistema operativo se utilizarán para transferir los archivos solo si las herramientas del Agente de red no están disponibles.

  Está opción se habilita de manera predeterminada para las tareas de instalación remota creadas en servidores de administración virtuales.

- **Con los recursos del sistema operativo a través del Servidor de administración**

  Si se habilita esta opción, los archivos se transmitirán a los dispositivos cliente a través del Servidor de administración utilizando las herramientas provistas por el sistema operativo de los dispositivos cliente. Puede habilitar esta opción si no hay ningún Agente de red instalado en el dispositivo cliente, pero el dispositivo cliente está en la misma red que el Servidor de administración.

  Esta opción está activada de forma predeterminada.

Configure las opciones adicionales:

- **No reinstalar la aplicación si ya está instalada**

  Si habilita esta opción y se detecta que la aplicación ya está instalada en el dispositivo cliente, no se la reinstalará.

  Si no habilita esta opción, la aplicación se instalará en todos los casos.

  Esta opción está activada de forma predeterminada.

- **Asignar la instalación del paquete en las directivas de grupo de Active Directory**

  Si se habilita esta opción, se instala un paquete de instalación mediante las directivas de grupo de Active Directory.

  Esta opción se encuentra disponible si se selecciona el paquete de instalación del Agente de red.

  Esta opción está deshabilitada de forma predeterminada.

# Paso 7. Opciones de reinicio

Indique qué acción se llevará a cabo si se necesita reiniciar el sistema operativo al instalar la aplicación:

- **No reiniciar el dispositivo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

- **Reiniciar el dispositivo**

  Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

  Esta opción está seleccionada de forma predeterminada.

  - **Repetir solicitud cada (min)**

    Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

    Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

    Si no habilita esta opción, la solicitud se mostrará una sola vez.

  - **Reiniciar después de (min)**

    Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

    Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de aplicaciones en sesiones bloqueadas**

  Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

  Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

  Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

  Esta opción está deshabilitada de forma predeterminada.

# Paso 8. Eliminar aplicaciones incompatibles antes de la instalación

Verá este paso únicamente si se tiene constancia de que la aplicación que se va a desplegar es incompatible con otras aplicaciones.

Seleccione la opción si desea que Kaspersky Security Center elimine automáticamente aplicaciones que sean incompatibles con la aplicación que despliegue.

También se muestra la lista de aplicaciones incompatibles.

Si no selecciona la opción, la aplicación se instalará únicamente en aquellos dispositivos que no tengan aplicaciones incompatibles.

## Paso 9. Mover los dispositivos a Dispositivos administrados

Indique si los dispositivos deberán moverse a un grupo de administración después de la instalación del Agente de red.

- **No mover los dispositivos**

  Los dispositivos se mantendrán en los grupos en los que se encuentren. Los dispositivos que no pertenezcan a ningún grupo quedarán sin asignar.

- **Mover los dispositivos no asignados a un grupo**

  Los dispositivos se moverán al grupo de administración que seleccione.

La opción **No mover los dispositivos** está seleccionada de manera predeterminada. Es posible que quiera mover los dispositivos manualmente por seguridad.

## Paso 10. Seleccionar cuentas con acceso a los dispositivos

De ser necesario, agregue las cuentas que se utilizarán para iniciar la tarea de instalación remota:

- **No se necesita una cuenta (el Agente de red está instalado)**

  Si selecciona esta opción, no necesitará especificar la cuenta con la que se ejecutará el instalador de la aplicación. Para ejecutar la tarea, se usará la cuenta con la que se haya iniciado el servicio del Servidor de administración.

  Esta opción no está disponible si el Agente de red no se instaló en los dispositivos cliente.

- **Se necesita una cuenta (no se utiliza el Agente de red)**

Seleccione esta opción si el Agente de red no está instalado en los dispositivos a los que asigna la tarea de instalación remota. En este caso, puede especificar una cuenta de usuario o un certificado SSH para instalar la aplicación.

- **Cuenta local**. Si se selecciona esta opción, especifique la cuenta bajo la que se ejecutará el instalador de aplicación. Haga clic en el botón **Agregar**, seleccione **Cuenta local** y, a continuación, especifique las credenciales de la cuenta de usuario.

  Puede especificar varias cuentas de usuario si, por ejemplo, ninguna de ellas tiene todos los derechos requeridos en todos los dispositivos a los que asigne esta tarea. En este caso, todas las cuentas añadidas se utilizan para ejecutar la tarea, en orden consecutivo de arriba abajo.

- **Certificado de SSH**. Si desea instalar una aplicación en un dispositivo cliente basado en Linux, puede especificar un certificado SSH en lugar de una cuenta de usuario. Haga clic en el botón **Agregar**, seleccione **Certificado de SSH** y, a continuación, especifique las claves pública y privada del certificado.

  Para generar una clave privada, puede utilizar la utilidad ssh-keygen. Tenga en cuenta que Kaspersky Security Center espera que la clave privada esté en formato PEM, pero, de manera predeterminada, la utilidad ssh-keygen genera claves SSH en formato OPENSSH. Kaspersky Security Center no admite el formato OPENSSH. Para crear una clave privada en el formato PEM admitido, agregue la opción -m PEM en el comando ssh-keygen. Por ejemplo:

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "<correo electrónico del usuario>"
  ```

## Paso 11. Inicio de la instalación

Esta página es el último paso del asistente. En este paso, la tarea **Tarea de instalación remota** está correctamente creada y configurada.

De manera predeterminada, la opción **Ejecutar la tarea al finalizar el asistente** no está seleccionada. Si selecciona esta opción, la tarea **Tarea de instalación remota** comenzará inmediatamente después de que complete el asistente. Si no selecciona esta opción, la tarea **Tarea de instalación remota** no comenzará. Podrá iniciar la tarea manualmente cuando lo desee.

Haga clic en **Aceptar** para completar el paso final del Asistente de despliegue de la protección.

# Despliegue de aplicaciones de Kaspersky a través de Kaspersky Security Center Web Console

En esta sección se describe cómo puede usar Kaspersky Security Center Web Console para desplegar las aplicaciones de Kaspersky en los dispositivos cliente de su organización.

# Escenario: despliegue de aplicaciones de Kaspersky a través de Kaspersky Security Center Web Console

En este tema, se explica cómo desplegar aplicaciones de Kaspersky por medio de Kaspersky Security Center Web Console. Puede utilizar el Asistente de inicio rápido y el Asistente de despliegue de la protección, o puede completar todos los pasos manualmente.

Las siguientes aplicaciones pueden desplegarse a través de Kaspersky Security Center Web Console:

- Kaspersky Endpoint Security para Windows
- Kaspersky Endpoint Security for Linux

## Etapas

El despliegue de las aplicaciones de Kaspersky se divide en etapas:

1. **Descargar complemento de administración para la aplicación**

   Esta etapa puede completarse con el asistente de inicio rápido. Si elige no ejecutar el asistente, descargue el complemento para Kaspersky Endpoint Security para Windows manualmente.

   Si planea administrar dispositivos móviles corporativos, siga las instrucciones proporcionadas en la Ayuda de Kaspersky Security for Mobile para descargar e instalar los complementos de administración de Kaspersky Endpoint Security para Android.

2. **Descarga y creación de paquetes de instalación**

   Esta etapa puede completarse con el asistente de inicio rápido.

   El Asistente de inicio rápido permite descargar el paquete de instalación con el complemento de administración. Si no seleccionó esta opción al utilizar el asistente, o si sencillamente no utilizó el Asistente, descargue el paquete manualmente.

   Si no puede instalar aplicaciones de Kaspersky por medio de Kaspersky Security Center en algunos dispositivos, por ejemplo, en dispositivos remotos de empleados, puede crear paquetes de instalación independientes para las aplicaciones. Si usa paquetes independientes para instalar aplicaciones de Kaspersky, no tiene que crear y ejecutar una tarea de instalación remota, ni crear y configurar tareas para Kaspersky Endpoint Security para Windows.

3. **Creación, configuración y ejecución de la tarea de instalación remota**

   Para Kaspersky Endpoint Security para Windows, esta etapa es parte del Asistente de despliegue de la protección, que se inicia automáticamente una vez que el Asistente de inicio rápido ha finalizado. Si opta por no ejecutar el Asistente de despliegue de la protección, cree esta tarea y configúrela manualmente.

   También puede crear manualmente varias tareas de instalación remotas para grupos de administración diferentes o selecciones de dispositivos diferentes. Puede desplegar diferentes versiones de una aplicación en estas tareas.

   Asegúrese de que todos los dispositivos de la red se hayan descubierto; a continuación, ejecute la tarea (o las tareas) de instalación remota.

   > Instale la utilidad nmap en sus activos basados en Linux. Esta utilidad es necesaria para habilitar la funcionalidad Reconocimiento de ubicación de red.

Si desea instalar el Agente de red en dispositivos con el sistema operativo SUSE Linux Enterprise Server 15, primero, instale el paquete insserv-compat para configurar el Agente de red.

Si desea instalar el Agente de Red en dispositivos que utilicen el sistema operativo RED OS 7.3.4 o posterior, o MSVSPHERE 9.2 o posterior, instale el paquete libxcrypt-compat para el correcto funcionamiento del Agente de Red.

4. **Creación y configuración de tareas para la aplicación administrada**

   La tarea *Instalar actualización* de Kaspersky Endpoint Security para Windows debe estar configurada.

   Esta etapa forma parte del Asistente de inicio rápido: la tarea se crea y configura automáticamente con la configuración predeterminada. Si opta por no ejecutar el asistente, cree esta tarea y configúrela manualmente. Si utiliza el Asistente de inicio rápido, asegúrese de que la programación de la tarea cumpla con sus requisitos. (De manera predeterminada, el inicio programado para la tarea se establece en **Manualmente**, pero es posible que desee elegir otra opción).

   Otras aplicaciones de Kaspersky podrían tener otras tareas predeterminadas. Por favor, consulte la documentación de las aplicaciones correspondientes para más información.

   Asegúrese de que la programación para cada tarea que crea que cumpla con sus requisitos.

5. **Instalación de Kaspersky Security for Mobile (opcional)**

   Si planea administrar dispositivos móviles corporativos, siga las instrucciones que se brindan en la Ayuda de Kaspersky Security para dispositivos móviles. Allí encontrará información sobre el despliegue de Kaspersky Endpoint Security para Android.

6. **Creando directivas**

   Cree la directiva para cada aplicación manualmente o (en el caso de Kaspersky Endpoint Security para Windows) a través del Asistente de inicio rápido. Puede utilizar la configuración predeterminada de la directiva; también puede modificar la configuración predeterminada de la directiva de acuerdo con sus necesidades en cualquier momento.

7. **Verificación de los resultados**

   Asegúrese de que la distribución se completó correctamente: tiene directivas y tareas para cada aplicación y estas aplicaciones están instaladas en los dispositivos administrados.

### Resultados

Completar las etapas anteriores tiene los siguientes resultados:

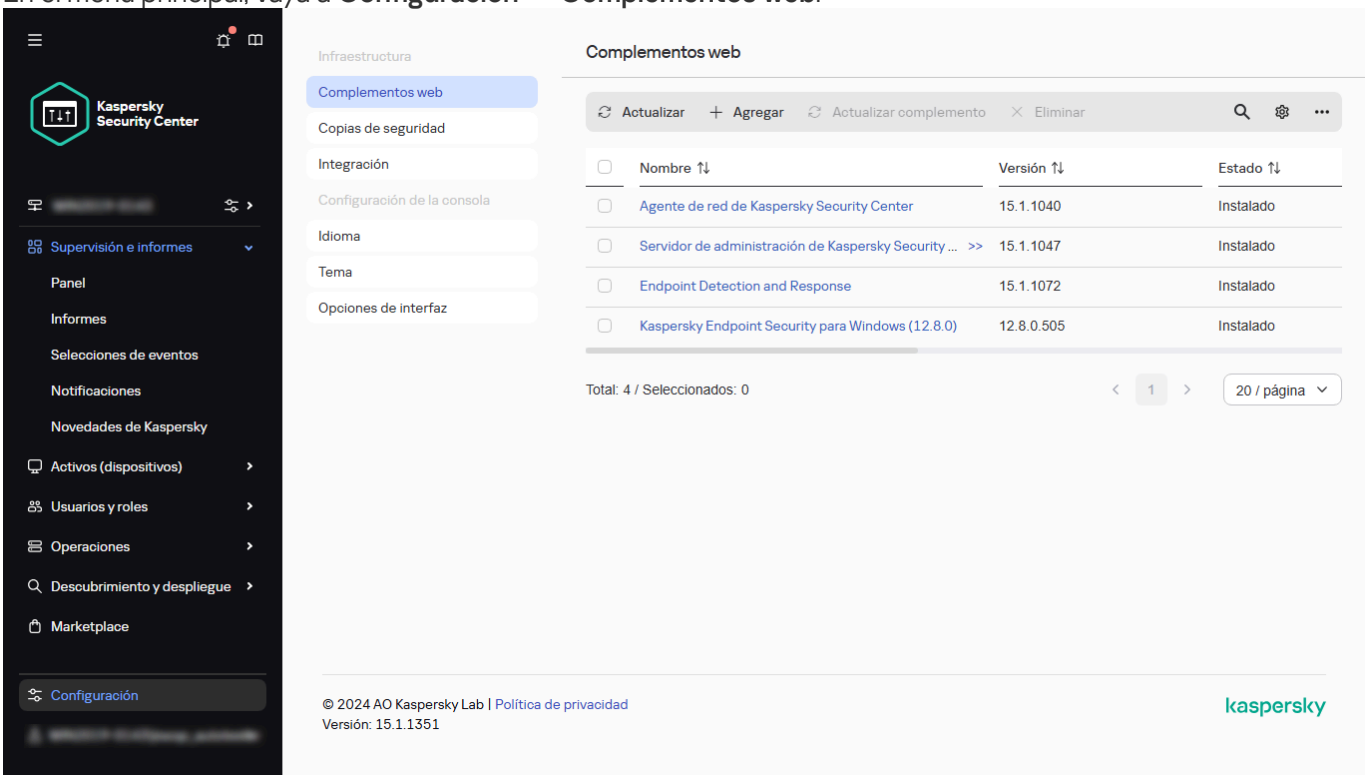
- Se crean todas las directivas y tareas necesarias para las aplicaciones seleccionadas.
- Los horarios de las tareas se configuran de acuerdo a sus necesidades.
- Las aplicaciones seleccionadas se despliegan o programan para desplegarse en los dispositivos cliente seleccionados.

## La adquisición de complementos para aplicaciones de Kaspersky

Para desplegar una aplicación Kaspersky, como Kaspersky Endpoint Security para Windows, debe descargar el complemento de administración de la aplicación.

*Para descargar un complemento de administración para una aplicación de Kaspersky:*

1. En el menú principal, vaya a **Configuración → Complementos web**.




La lista de complementos web instalados

2. En la ventana que se abre, haga clic en el botón **Agregar**.

   Se muestra una lista de complementos disponibles.

3. En la lista de complementos disponibles, seleccione el complemento que desea descargar (por ejemplo, Kaspersky Endpoint Security 11 para Windows) haciendo clic en su nombre.

   Se muestra una página de descripción del complemento.

4. En la página de descripción del complemento, haga clic en **Instale el complemento**.

5. Cuando la instalación se haya completado, haga clic en **Aceptar**.

El complemento de administración se descarga con la configuración predeterminada y se muestra en la lista de complementos de administración.

Puede agregar complementos y actualizar los complementos descargados desde un archivo. Puede descargar los complementos de administración y los complementos de administración web desde la página web del Servicio de soporte técnico de Kaspersky.

*Para descargar o actualizar complementos desde un archivo, siga estos pasos:*

1. En el menú principal, vaya a **Configuración → Complementos web**.

2. Realice una de las siguientes acciones:

   - Haga clic en **Agregar desde archivo** para descargar un complemento desde un archivo.
   - Haga clic en **Actualizar desde archivo** para descargar la actualización de un complemento desde un archivo.

3. Especifique el archivo y la firma del archivo.

4. Descargue los archivos especificados.

   El complemento de administración se descarga del archivo y se muestra en la lista de complementos de administración.

# Descargar y crear paquetes de instalación para aplicaciones de Kaspersky

Puede crear paquetes de instalación de aplicaciones de Kaspersky desde los servidores web de Kaspersky si su Servidor de administración tiene acceso a Internet.

*Para descargar y crear un paquete de instalación para una aplicación de Kaspersky:*

1. Realice una de las siguientes acciones:

   - En el menú principal, vaya a **Descubrimiento y despliegue** → **Despliegue y asignación** → **Paquetes de instalación**.
   - En el menú principal, vaya a **Operaciones** → **Repositorios** → **Paquetes de instalación**.

   También puede ver las notificaciones sobre nuevos paquetes para aplicaciones de Kaspersky en la lista de notificaciones en pantalla. Si la lista contiene notificaciones sobre un nuevo paquete, haga clic en el vínculo ubicado junto a una notificación para abrir la lista de paquetes de instalación disponibles.

   Se muestra una lista de paquetes de instalación disponibles en el Servidor de administración.

2. Haga clic en **Agregar**.

   Se inicia el Asistente de nuevo paquete. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. Seleccione **Crear un paquete de instalación para una aplicación de Kaspersky**.

   Aparecerá una lista de paquetes de instalación disponibles en los servidores web de Kaspersky. La lista contiene paquetes de instalación solo para aquellas aplicaciones que son compatibles con la versión actual de Kaspersky Security Center.

4. Haga clic en el nombre de un paquete de instalación, por ejemplo, Kaspersky Endpoint Security para Windows (11.1.0).

   Se abrirá una ventana con información sobre el paquete de instalación.

   Si esto se ajusta a las leyes y normativas aplicables, puede descargar y usar un paquete de instalación que incluya herramientas criptográficas que implementen un estándar de cifrado fuerte. Para descargar un paquete de distribución de Kaspersky Endpoint Security para Windows que sea adecuado para las necesidades de su organización, consulte la legislación del país donde se encuentren los dispositivos cliente de su organización.

5. Lea la información y haga clic en el botón **Descargar y crear paquete de instalación**.

   Si no se puede convertir un paquete de distribución en uno de instalación, se mostrará el botón **Descargar paquete de distribución** en lugar de **Descargar y crear paquete de instalación**.

   Comenzará el proceso para descargar el paquete de instalación al Servidor de administración. Puede cerrar la ventana del asistente o avanzar al siguiente paso de las instrucciones. Si cierra la ventana del asistente, la descarga continuará en segundo plano.

   Si desea controlar la descarga del paquete de instalación:

   a. En el menú principal, vaya a **Operaciones** → **Repositorios** → **Paquetes de instalación** → **En curso ()**.

   b. Consulte las columnas **Progreso de la descarga** y **Estado de descarga** de la tabla para seguir el progreso de la operación.

   Cuando se complete la descarga, el paquete de instalación aparecerá en la lista de la pestaña **Descargado**. Si la descarga se detiene y el estado de descarga cambia a **Aceptar EULA**, haga clic en el nombre del paquete de instalación y avance al siguiente paso de las instrucciones.

   > Si selecciona un paquete de distribución que contenga un volumen de datos mayor de lo admisible, verá un mensaje de error. Para que la aplicación le permita crear el paquete de instalación, deberá modificar el límite pertinente.

6. Para algunas aplicaciones de Kaspersky, durante el proceso de descarga, se muestra el botón **Mostrar EULA**. Si ve este botón, haga lo siguiente:

   a. Haga clic en el botón **Mostrar EULA** para leer el Contrato de licencia de usuario final (EULA).

   b. Lea el EULA que aparece en pantalla y haga clic en **Aceptar**.

      La descarga continúa después de aceptar el EULA. Si hace clic en **Rechazar**, la descarga se detiene.

7. Cuando se complete la descarga, haga clic en el botón **Cerrar**.

El paquete de instalación seleccionado se descargará a la subcarpeta Packages de la carpeta compartida del Servidor de administración. Cuando termine la descarga, el paquete de instalación aparecerá en la lista de paquetes de instalación.

# Modificación del límite de datos para paquetes de instalación personalizados

Existe un límite a la cantidad de datos que se admite descomprimir para crear un paquete de instalación personalizado. El límite predeterminado es 1 GB.

Si intenta cargar un archivo de almacenamiento que contenga un volumen de datos superior a lo permitido, verá un mensaje de error. Por ello, para crear un paquete de instalación a partir de un paquete de distribución de gran tamaño, puede ser necesario aumentar el límite predeterminado.

*Para cambiar el límite de datos para paquetes de instalación personalizados:*

1. En el dispositivo del Servidor de administración, abra la línea de comandos con la cuenta que se haya usado para instalar el Servidor de administración.

2. Cambie de directorio a la carpeta de instalación de Kaspersky Security Center (generalmente, C:\Archivos de programa (x86)\Kaspersky Lab\Kaspersky Security Center).

3. Dependiendo de cómo se haya instalado el Servidor de administración, ejecute uno de los siguientes comandos con derechos de administrador:

   - Instalación local normal:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <número de bytes>
     ```

   - Instalación en el clúster de conmutación por error de Kaspersky Security Center:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <número de bytes> --stp klfoc
     ```

   - Instalación en un clúster de conmutación por error de Windows Server:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <número de bytes> --stp cluster
     ```

   El valor de <número de bytes> debe ser un número de bytes en formato decimal o hexadecimal.

   Por ejemplo, si el límite requerido es de 2 GB, puede especificar el valor decimal 2147483648 o el valor hexadecimal 0x80000000. Así, para una instalación local del Servidor de administración, usaría el siguiente comando:

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

La aplicación comenzará a usar el nuevo límite de datos para los paquetes de instalación personalizados.

# Descargar paquetes de distribución para aplicaciones de Kaspersky

En Kaspersky Security Center Web Console, puede descargar y guardar paquetes de distribución para las aplicaciones de Kaspersky. Puede usar los paquetes de distribución para instalar las aplicaciones manualmente, sin usar Kaspersky Security Center.

*Para descargar y guardar paquetes de distribución para aplicaciones de Kaspersky:*

1. En el menú principal, vaya a **Operaciones** → **Aplicaciones Kaspersky** → **Versiones actuales de la aplicación**.

   Se abrirá la lista de paquetes de distribución, complementos y revisiones disponibles. Kaspersky Security Center muestra solo los elementos que son compatibles con su versión actual.

2. En la lista, haga clic en el nombre del paquete que desea descargar.

   Se abre la descripción del paquete.

3. Lea la descripción y haga clic en el botón **Descargar y crear paquete de instalación**.

   Si no se puede convertir un paquete de distribución en uno de instalación, se mostrará el botón **Descargar paquete de distribución** en lugar de **Descargar y crear paquete de instalación**.

   El paquete de instalación se descargará al Servidor de administración.

El paquete de instalación o de distribución seleccionado se descargará a la subcarpeta **Packages** de la carpeta compartida del Servidor de administración. Cuando termine la descarga, el paquete de instalación aparecerá en la lista de paquetes de instalación.

# Verificar que Kaspersky Endpoint Security se haya desplegado correctamente

*Para asegurarse de que ha desplegado correctamente las aplicaciones de Kaspersky, como Kaspersky Endpoint Security:*

1. Con Kaspersky Security Center Web Console, asegúrese de tener lo siguiente:
   - Una directiva para Kaspersky Endpoint Security y/u otras aplicaciones de seguridad que utilice.
   - Tareas para Kaspersky Endpoint Security para Windows: tarea *Análisis rápido* y tarea *Instalar actualización* (si utiliza Kaspersky Endpoint Security para Windows).
   - Las tareas para otras aplicaciones de la seguridad que utiliza.
2. En uno de los dispositivos administrados, seleccionados para la instalación, asegúrese de lo siguiente:
   - Kaspersky Endpoint Security u otra aplicación de seguridad de Kaspersky está instalada.
   - En Kaspersky Endpoint Security, la protección contra archivos peligrosos, la protección contra amenazas web y la protección contra amenazas de correo coinciden con la directiva que creó para este dispositivo.
   - El servicio Kaspersky Endpoint Security se puede detener e iniciar manualmente.
   - Las tareas de grupo se pueden detener e iniciar manualmente.

# Creación de paquetes de instalación independientes

Usted y los usuarios de dispositivos de su organización pueden utilizar paquetes de instalación independientes para instalar aplicaciones en dispositivos de forma manual.

Un paquete de instalación independiente es un archivo ejecutable (installer.exe) que puede almacenar en el Servidor web o en una carpeta compartida, enviar por correo electrónico o transferir al dispositivo cliente mediante algún otro método. En el dispositivo cliente, el usuario puede ejecutar el archivo recibido localmente para instalar una aplicación sin utilizar Kaspersky Security Center. Puede crear paquetes de instalación independientes de aplicaciones de Kaspersky y de aplicaciones de terceros para plataformas Windows, macOS y Linux. Para crear un paquete de instalación independiente para una aplicación de terceros, debe crear un paquete de instalación personalizada.

Asegúrese de que el paquete de instalación independiente no esté disponible para personas no autorizadas.

*Para crear un paquete de instalación independiente:*

1. Realice una de las siguientes acciones:

   - En el menú principal, vaya a **Descubrimiento y despliegue → Despliegue y asignación → Paquetes de instalación**.
   - En el menú principal, vaya a **Operaciones → Repositorios → Paquetes de instalación**.

   Se muestra una lista de paquetes de instalación disponibles en el Servidor de administración.

2. En la lista de paquetes de instalación, seleccione un paquete de instalación y haga clic en el botón **Desplegar** que se encuentra arriba de la lista.

3. Seleccione la opción **Usar un paquete independiente**.

   Se inicia el asistente de creación de paquetes de instalación independiente. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

4. Asegúrese de que la opción **Instalar el Agente de red junto con esta aplicación** esté habilitada si desea instalar el Agente de red junto con la aplicación seleccionada.

   > La opción se muestra dependiendo de la aplicación para la que cree un paquete de instalación independiente.

   Esta opción está activada de forma predeterminada. Recomendamos que active esta opción si no sabe si el Agente de red está instalado en el dispositivo. Si el Agente de red ya está instalado en el dispositivo, una vez que instale el paquete de instalación independiente con el Agente de red, este último se actualizará a la versión más reciente.

   Si deshabilita esta opción, el Agente de red no se instalará en el dispositivo, y el dispositivo quedará como dispositivo no administrado.

   El asistente le indicará si el Servidor de administración ya cuenta con un paquete de instalación independiente para la aplicación seleccionada. Si esto sucede, elija una de estas acciones:

   - **Crear un paquete de instalación independiente**. Seleccione esta opción si, por ejemplo, desea crear un paquete de instalación independiente para una nueva versión de la aplicación y también conservar un paquete de instalación independiente que haya creado para una versión de la aplicación anterior. El nuevo paquete de instalación independiente se ubicará en otra carpeta.
   - **Utilizar un paquete de instalación independiente que ya existe**. Seleccione esta opción si desea utilizar un paquete de instalación independiente que ya exista. El proceso para crear paquetes no se iniciará.
   - **Volver a generar un paquete de instalación independiente que ya existe**. Seleccione esta opción si desea volver a crear un paquete de instalación independiente para la misma aplicación. El paquete de instalación independiente se ubicará en la misma carpeta.

5. En el paso **Mover a lista de dispositivos administrados**, la opción **No mover los dispositivos** está habilitada de manera predeterminada. Si no desea mover el dispositivo cliente a ningún grupo de administración después de la instalación del Agente de red, deje la opción habilitada.

   Si desea mover el dispositivo cliente después de la instalación del Agente de red, seleccione la opción **Mover los dispositivos no asignados a este grupo** y especifique el grupo de administración al que desea mover el dispositivo cliente. De forma predeterminada, el dispositivo se moverá al grupo **Dispositivos administrados**.

6. Cuando finalice el proceso de creación del paquete de instalación independiente, haga clic en el botón **FINALIZAR**.

   Se cierra el Asistente de creación de un paquete de instalación independiente.

Se crea el paquete de instalación independiente y se lo ubica en la subcarpeta PkgInst de la carpeta compartida del Servidor de administración. Puede ver la lista de paquetes independientes si hace clic en el botón **Ver la lista de paquetes independientes** que se encuentra arriba de la lista de paquetes de instalación.

# Ver la lista de paquetes de instalación independientes

Puede ver la lista de paquetes de instalación independientes y las propiedades de cada paquete.

*Para ver la lista de paquetes de instalación independientes para todos los paquetes de instalación:*

Haga clic en el botón **Ver la lista de paquetes independientes**, ubicado encima de la lista.

En la lista de paquetes de instalación independientes, sus propiedades se muestran de la siguiente manera:

- **Nombre del paquete**. Nombre del paquete de instalación independiente. Se crea automáticamente a con el nombre y la versión de la aplicación incluida en el paquete.
- **Nombre de la aplicación**. Es el nombre de la aplicación que se incluye en el paquete de instalación independiente.
- **Versión de la aplicación**.
- **Nombre del paquete de instalación del Agente de red**. La propiedad se muestra únicamente si el Agente de red está incluido en el paquete de instalación independiente.
- **Versión del Agente de red**. La propiedad se muestra únicamente si el Agente de red está incluido en el paquete de instalación independiente.
- **Tamaño**. Tamaño del archivo en MB.
- **Grupo**. Nombre del grupo al que se mueve el dispositivo cliente después de la instalación del Agente de red.
- **Creado**. Fecha y hora de creación del paquete de instalación independiente.
- **Modificado**. Fecha y hora de modificación del paquete de instalación independiente.
- **Ruta**. Ruta completa a la carpeta donde se encuentra el paquete de instalación independiente.
- **Dirección web**. Dirección web de la ubicación del paquete de instalación independiente.
- **Hash de archivo**. La propiedad se utiliza para certificar que ningún tercero haya modificado el paquete de instalación independiente y que un usuario tiene el mismo archivo que usted creó y transfirió al usuario.

*Para ver la lista de paquetes de instalación independientes para un paquete de instalación específico:*

Seleccione el paquete de instalación de la lista y, a continuación, haga clic en el botón **Ver la lista de paquetes independientes** ubicado encima de la lista.

En la lista de paquetes de instalación independientes puede hacer lo siguiente:

- Publicar un paquete de instalación independiente en el servidor web haciendo clic en el botón **Publicar**. El paquete de instalación independiente publicado está disponible para que lo descarguen los usuarios a quienes envió el vínculo.
- Cancelar la publicación de un paquete de instalación independiente en el servidor web haciendo clic en el botón **Cancelar la publicación**. El paquete de instalación independiente no publicado está disponible para que lo descargue solo usted y otros administradores.
- Descargar un paquete de instalación independiente a su dispositivo haciendo clic en el botón **Descargar**.
- Enviar un correo electrónico con el vínculo para un paquete de instalación independiente haciendo clic en el botón **Enviar por correo electrónico**.
- Eliminar un paquete de instalación independiente haciendo clic en el botón **Eliminar**.

# Crear un paquete de instalación personalizado

Puede utilizar paquetes de instalación personalizada para hacer lo siguiente:

- Para instalar cualquier aplicación (como un editor de texto) en un dispositivo cliente, por ejemplo, mediante una tarea.
- para crear un paquete de instalación independiente.

Un paquete de instalación personalizada es una carpeta con un conjunto de archivos. La fuente para crear un paquete de instalación personalizada es un *archivo de almacenamiento*. El archivo de almacenamiento contiene un archivo o archivos que deben incluirse en el paquete de instalación personalizada. Al crear un paquete de instalación personalizada, puede especificar parámetros de línea de comandos, por ejemplo, para instalar la aplicación en modo silencioso.

Si tiene una clave de licencia activa para la función Administración de vulnerabilidades y parches (VAPM), puede convertir la configuración de instalación predeterminada para el paquete de instalación personalizada relevante y usar los valores recomendados por los expertos de Kaspersky. La configuración se convierte automáticamente durante la creación del paquete de instalación personalizada solo si el archivo ejecutable correspondiente está incluido en la base de datos de Kaspersky de aplicaciones de terceros.

*Para crear un paquete de instalación personalizado:*

1. Realice una de las siguientes acciones:

   - En el menú principal, vaya a **Descubrimiento y despliegue** → **Despliegue y asignación** → **Paquetes de instalación**.
   - En el menú principal, vaya a **Operaciones** → **Repositorios** → **Paquetes de instalación**.

   Se muestra una lista de paquetes de instalación disponibles en el Servidor de administración.

2. Haga clic en **Agregar**.

   Se inicia el Asistente de nuevo paquete. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. Seleccione **Crear un paquete de instalación a partir de un archivo**.

4. Especifique el nombre del paquete y haga clic en el botón **Examinar**.

   Se abre una ventana estándar de Windows **Abrir** en su navegador para que elija un archivo para crear el paquete de instalación.

5. Elija un archivo de almacenamiento ubicado en los discos disponibles.

   Puede cargar un archivo comprimido ZIP, CAB, TAR o TAR.GZ. No es posible crear un paquete de instalación a partir de un archivo autoextraíble SFX.

   > Si desea que la configuración se convierta durante la instalación del paquete, asegúrese de que la casilla **Al finalizar el asistente, convertir los valores de configuración a los recomendados para las aplicaciones que reconoce Kaspersky Security Center** esté seleccionada y haga clic en **Siguiente**.

   Se inicia la carga de archivos al Servidor de administración de Kaspersky Security Center.

   > Si habilitó el uso de la configuración de instalación recomendada, Kaspersky Security Center 15.1 verifica si el archivo ejecutable está incluido en la base de datos de Kaspersky de aplicaciones de terceros. Si la verificación arroja un resultado positivo, recibirá una notificación que le informará que se reconoció el archivo. Se convierte la configuración y se crea el paquete de instalación personalizada. No se requieren más acciones. Haga clic en el botón **Finalizar** para cerrar el asistente.

6. Seleccione un archivo (de la lista de archivos que se extraen del archivo de almacenamiento elegido) y especifique los parámetros de la línea de comandos de un archivo ejecutable.

   Puede especificar parámetros de línea de comandos para instalar la aplicación desde el paquete de instalación en modo silencioso. La especificación de los parámetros de la línea de comandos es opcional.

   Se inicia el proceso para crear el paquete de instalación.

   El asistente le informará cuando finalice el proceso.

   Si no se crea el paquete de instalación, se muestra el mensaje pertinente.

7. Haga clic en el botón **Finalizar** para cerrar el asistente.

El paquete de instalación que ha creado se descarga en la subcarpeta Paquetes de la carpeta compartida del Servidor de administración. Al concluir la descarga, el paquete de instalación aparecerá en la lista de paquetes de instalación.

En la lista de paquetes de instalación disponibles en el Servidor de administración, al hacer clic en el vínculo con el nombre de un paquete de instalación personalizado, puede hacer lo siguiente:

- Ver las siguientes propiedades del paquete de instalación:
  - **Nombre**. Nombre del paquete de instalación personalizado.
  - **Origen**. Nombre del proveedor de la aplicación.
  - **Aplicación**: Nombre de la aplicación que contiene el paquete de instalación personalizado.
  - **Versión**. Versión de la aplicación.
  - **Idioma**. Idioma de la aplicación que contiene el paquete de instalación personalizado.
  - **Tamaño (MB)**. Tamaño del paquete de instalación.
  - **Sistema operativo**. Tipo de sistema operativo para el que está destinado el paquete de instalación.
  - **Creado**. Fecha de creación del paquete de instalación.
  - **Modificado**. Fecha de modificación del paquete de instalación.
  - **Tipo**. Tipo de paquete de instalación.
- Cambie el nombre del paquete y los parámetros de la línea de comandos. Esta función solo está disponible para los paquetes que no se crean sobre la base de las aplicaciones de Kaspersky.

Si ha convertido la configuración de instalación del paquete de instalación a los valores recomendados para el proceso de creación del paquete personalizado, pueden aparecer dos secciones adicionales en la pestaña **Configuración** de las propiedades del paquete de instalación personalizada: **Configuración** y **Procedimiento de instalación**.

La sección **Configuración** contiene las siguientes propiedades, que se muestran en una tabla:

- **Nombre**. En esta columna, se muestra el nombre asignado a un parámetro de instalación.
- **Tipo**. En esta columna, se muestra el tipo del parámetro de instalación.
- **Valor**. En esta columna, se muestra el tipo de datos definidos por un parámetro de instalación (Booleano, Ruta de archivo, Numérico, Ruta o Cadena).

La sección **Procedimiento de instalación** contiene una tabla en la que se describen las siguientes propiedades de la actualización incluida en el paquete de instalación personalizada:

- **Nombre**. Nombre de la actualización.
- **Descripción**. Descripción de la actualización.
- **Fuente**. La fuente de la actualización, es decir, si la lanzó Microsoft o un desarrollador externo diferente.
- **Tipo**. El tipo de actualización, es decir, si la actualización está destinada a un controlador o una aplicación.

- **Categoría**. La categoría de Windows Server Update Services (WSUS) que se muestra para las actualizaciones de Microsoft (Actualizaciones críticas, Actualizaciones de las definiciones, Controladores, Paquetes de características, Actualizaciones de seguridad, Service Packs, Herramientas, Paquetes acumulativos de actualizaciones, Actualizaciones o Upgrade).
- **Nivel de importancia conforme a MSRC**. El nivel de importancia de la actualización definido por Microsoft Security Response Center (MSRC).
- **Nivel de importancia**. El nivel de importancia de la actualización definido por Kaspersky.
- **Nivel de importancia del parche (parches previstos para las aplicaciones de Kaspersky)**. El nivel de importancia del parche si está destinado para una aplicación de Kaspersky.
- **Artículo**. El identificador (id.) del artículo de la Base de conocimientos que describe la actualización.
- **Boletín**. El id. del boletín de seguridad que describe la actualización.
- **Instalación no asignada**. Muestra si la actualización tiene el estado Instalación no asignada.
- **Por instalarse**. Muestra si la actualización tiene el estado Por instalarse.
- **Instalándose**. Muestra si la actualización tiene el estado Instalando.
- **Instalada**. Muestra si la actualización tiene el estado Instalada.
- **Error**. Muestra si la actualización tiene el estado Error.
- **Se debe reiniciar el dispositivo**. Muestra si la actualización tiene el estado Se debe reiniciar el dispositivo.
- **Registrado**. Muestra la fecha y hora en que se registró la actualización.
- **Instalada en modo interactivo**. Muestra si la actualización solicita una interacción con el usuario durante la instalación.
- **Revocado**. Muestra la fecha y hora en que se revocó la actualización.
- **Estado de aprobación de la actualización**. Muestra si la instalación de la actualización está aprobada.
- **Revisión**. Muestra el número de revisión actual de la actualización.
- **Id. de actualización**. Muestra el id. de la actualización.
- **Versión de la aplicación**. Muestra el número de versión al que se actualizará la aplicación.
- **Reemplazada**. Muestra otras actualizaciones que pueden reemplazar a la actualización.
- **Reemplaza**. Muestra otras actualizaciones que pueden ser reemplazadas por la actualización.
- **Debe aceptar los términos del Contrato de licencia**. Muestra si la actualización solicita aceptar los términos de un contrato de licencia de usuario final (EULA).
- **Proveedor**. Muestra el nombre del proveedor de la actualización.
- **Familia de aplicaciones**. Muestra el nombre de la familia de aplicaciones a las que pertenece la actualización.
- **Aplicación**. Muestra el nombre de la aplicación a la que pertenece la actualización.

- **Idioma**. Muestra el idioma de la localización de la actualización.
- **Instalación no asignada (nueva versión)**. Muestra si la actualización tiene el estado Instalación no asignada (nueva versión).
- **Requiere instalación de requisitos previos**. Muestra si la actualización tiene el estado Requiere instalación de requisitos previos.
- **Modo de descarga**. Muestra el modo de descarga de la actualización.
- **Es un parche**. Muestra si la actualización es un parche.
- **Sin instalar**. Muestra si la actualización tiene el estado Sin instalar.

# Distribución de paquetes de instalación a servidores de administración secundarios

A través de Kaspersky Security Center Linux, puede crear paquetes de instalación para aplicaciones desarrolladas por Kaspersky y por terceros, distribuir paquetes de instalación a sus dispositivos cliente e instalar aplicaciones utilizando esos paquetes. Para optimizar la carga del Servidor de administración principal, puede distribuir los paquetes de instalación a los servidores de administración secundarios. Los servidores secundarios transmiten luego esos paquetes a los dispositivos cliente. Concluida la distribución, puede realizarse la instalación remota de las aplicaciones en los dispositivos cliente.

*Para distribuir paquetes de instalación a servidores de administración secundarios:*

1. Verifique que los servidores de administración secundarios estén conectados al Servidor de administración principal.
2. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.

   Se muestra la lista de tareas.
3. Haga clic en el botón **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.
4. En la página **Configuración de tarea nueva**, abra la lista desplegable **Aplicación** y seleccione **Kaspersky Security Center**. A continuación, en la lista desplegable **Tipo de tarea**, seleccione **Distribuir paquete de instalación**. Ingrese el nombre de la tarea.
5. En la página **Alcance de la tarea**, seleccione los dispositivos a los que se asigna la tarea de una de estas formas:
   - Si desea crear una tarea para todos los servidores de administración secundarios de un grupo de administración específico, seleccione ese grupo y cree una tarea de grupo para el mismo.
   - Si desea crear una tarea para determinados servidores de administración secundarios, seleccione esos servidores y cree una tarea para ellos.
6. En la página **Paquetes de instalación distribuidos**, seleccione los paquetes de instalación que se copiarán a los servidores de administración secundarios.

7. Seleccione la cuenta con la que se ejecutará la tarea *Distribuir paquete de instalación*. Puede usar su propia cuenta y dejar habilitada la opción **Cuenta predeterminada**. Como alternativa, puede elegir otra cuenta que tenga los derechos de acceso necesarios para ejecutar la tarea. Para ello, haga clic en **Especificar cuenta** e ingrese las credenciales de la cuenta que desee usar.

8. En la página **Finalizar la creación de la tarea**, puede habilitar la opción **Abrir los detalles de la tarea cuando se complete la creación** para que se abra la ventana de propiedades de la tarea y modificar, desde allí, la configuración de la tarea definida por defecto. Si lo prefiere, puede configurar los ajustes de la tarea en cualquier otro momento.

9. Haga clic en el botón **Finalizar**.

   En la lista de tareas, aparecerá la nueva tarea para distribuir los paquetes de instalación a los servidores de administración secundarios.

10. Ejecute la tarea manualmente o espere a que ocurra el inicio programado que haya definido en los ajustes.

    Una vez que se complete la tarea, los paquetes de instalación seleccionados estarán en los servidores de administración secundarios que haya seleccionado.

# Instalar aplicaciones mediante la tarea de instalación remota

Kaspersky Security Center permite que usted instale aplicaciones en dispositivos remotamente, usando las tareas de instalación remotas. Las tareas se crean y se asignan a los dispositivos a través de un asistente específico. Para asignar una tarea con mayor facilidad y rapidez, puede especificar los dispositivos (hasta 1000) de distintas maneras a través de la ventana del asistente:

- **Seleccionar dispositivos de la red detectados por el Servidor de administración**. En este caso, la tarea se asigna a dispositivos específicos. Estos pueden ser tanto dispositivos asignados a grupos de administración como dispositivos no asignados.

- **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**. Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

- **Asignar tarea a una selección de dispositivos**. En este caso, la tarea se asigna a los dispositivos incluidos en una selección creada anteriormente. Puede especificar la selección predeterminada o una personalizada que haya creado.

- **Asignar tarea a un grupo de administración**. En este caso, la tarea se asigna a los dispositivos incluidos en el grupo de administración creado anteriormente.

Para evitar problemas que puedan ocurrir durante la instalación de la aplicación en un dispositivo cliente sin Agente de red instalado, debe proceder como se describe en el despliegue forzado a través de la tarea de instalación remota de Kaspersky Security Center.

## Instalación de una aplicación de forma remota

Esta sección contiene información sobre cómo instalar una aplicación de forma remota en un grupo de administración, dispositivos con direcciones IP específicas o una selección de dispositivos administrados.

*Para instalar una aplicación en dispositivos específicos:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea.
3. En la sección **Tipo de tarea**, seleccione **Instalar aplicación de forma remota**.
4. Seleccione una de las siguientes opciones:

   - **Asignar tarea a un grupo de administración**

     La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

     Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

     Si la tarea se asigna a un grupo de administración, la pestaña **Seguridad** no se mostrará en la ventana de propiedades de la tarea; esto se debe a que las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

   - **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**

     Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

     Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.

   - **Asignar tarea a una selección de dispositivos**

     La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

     Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

   La tarea *Instalar aplicación de forma remota* se creará para los dispositivos especificados. Si seleccionó la opción **Asignar tarea a un grupo de administración**, la tarea será una tarea de grupo.
5. En el paso **Alcance de la tarea**, indique un grupo de administración, dispositivos con direcciones específicas o una selección de dispositivos.

   Los ajustes disponibles dependerán de la opción seleccionada en el paso anterior.

6. En el paso **Paquetes de instalación**, defina los siguientes ajustes:

- En el campo **Seleccionar paquete de instalación**, seleccione el paquete de instalación de la aplicación que desee instalar.
- En el grupo de configuraciones **Forzar la descarga del paquete de instalación**, puede especificar cómo se distribuyen a los dispositivos cliente los archivos que se requieren para la instalación de una aplicación:
  - **Con el Agente de red**

    Si habilita esta opción, los paquetes de instalación se transferirán a los dispositivos cliente a través del Agente de red instalado en esos dispositivos.

    Si no habilita esta opción, los paquetes de instalación se distribuirán utilizando las herramientas provistas por el sistema operativo de los dispositivos cliente.

    Recomendamos habilitar esta opción si la tarea está asignada a dispositivos que tienen instalado el Agente de red.

    Esta opción está habilitada de manera predeterminada.

  - **Con los recursos del sistema operativo a través de los puntos de distribución**

    Si habilita esta opción, los paquetes de instalación se transferirán a los dispositivos cliente mediante las herramientas del sistema operativo a través de los puntos de distribución. Puede seleccionar esta opción si existe al menos un punto de distribución en la red.

    Si habilitó la opción **Con el Agente de red**, las herramientas del sistema operativo se utilizarán para transferir los archivos solo si las herramientas del Agente de red no están disponibles.

    Está opción se habilita de manera predeterminada para las tareas de instalación remota creadas en servidores de administración virtuales.

  - **Con los recursos del sistema operativo a través del Servidor de administración**

    Si se habilita esta opción, los archivos se transmitirán a los dispositivos cliente a través del Servidor de administración utilizando las herramientas provistas por el sistema operativo de los dispositivos cliente. Puede habilitar esta opción si no hay ningún Agente de red instalado en el dispositivo cliente, pero el dispositivo cliente está en la misma red que el Servidor de administración.

    Esta opción está activada de forma predeterminada.

- En el campo **Número máximo de descargas simultáneas**, ingrese el número máximo permitido de dispositivos cliente a los que el Servidor de administración podrá transmitir simultáneamente los archivos.
- En el campo **Número máximo de intentos de instalación**, ingrese el límite de veces que se podrá ejecutar el instalador.

  Si se excede la cantidad de intentos especificados en el parámetro, Kaspersky Security Center deja de iniciar el instalador en el dispositivo. Para reiniciar la tarea *Instalar aplicación de forma remota*, aumente el valor del parámetro **Número máximo de intentos de instalación** e inicie la tarea. Como alternativa, cree una nueva tarea *Instalar aplicación de forma remota*.
- Si migra de una aplicación de Kaspersky a otra y su aplicación actual está protegida con contraseña, ingrese la contraseña en el campo **Contraseña para desinstalar la aplicación de Kaspersky actual**. Tenga en cuenta que, durante la migración, se desinstalará su aplicación de Kaspersky actual.

El campo **Contraseña para desinstalar la aplicación de Kaspersky actual** solo está disponible si seleccionó la opción **Con el Agente de red** en el grupo de configuración **Forzar la descarga del paquete de instalación**.

Puede usar la contraseña de desinstalación solo para la migración de Kaspersky Security para Windows Server a Kaspersky Endpoint Security para Windows al instalar Kaspersky Endpoint Security para Windows mediante la tarea *Instalar aplicación de forma remota*. El uso de la contraseña de desinstalación al instalar otros componentes puede causar errores de instalación.

Para completar el escenario de migración correctamente, asegúrese de que se cumplan los siguientes requisitos previos:

- Está utilizando el Agente de red de Kaspersky Security Center 14.2 para Windows o una versión posterior.
- Está instalando la aplicación en dispositivos con Windows.

- Defina la configuración adicional:
  - **No reinstalar la aplicación si ya está instalada**

    Si habilita esta opción y se detecta que la aplicación ya está instalada en el dispositivo cliente, no se la reinstalará.

    Si no habilita esta opción, la aplicación se instalará en todos los casos.

    Esta opción está activada de forma predeterminada.

  - **Verificar el tipo de sistema operativo antes de la descarga**

    Antes de transmitir los archivos a los dispositivos cliente, Kaspersky Security Center verifica si la configuración de la utilidad de Instalación puede aplicarse al sistema operativo del dispositivo cliente. Si la configuración no es corresponde, Kaspersky Security Center no transmite los archivos y no intenta instalar la aplicación. A modo de ejemplo, si necesita instalar una aplicación en los dispositivos de un grupo de administración que contenga dispositivos con sistemas operativos diferentes, puede asignar la tarea de instalación al grupo de administración y habilitar esta opción para que la tarea no afecte a aquellos dispositivos que no tengan el sistema operativo pertinente.

  - **Asignar la instalación del paquete en las directivas de grupo de Active Directory**

    Si se habilita esta opción, se instala un paquete de instalación mediante las directivas de grupo de Active Directory.

    Esta opción se encuentra disponible si se selecciona el paquete de instalación del Agente de red.

    Esta opción está deshabilitada de forma predeterminada.

  - **Solicitar a los usuarios que cierren las aplicaciones en ejecución**

Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

Esta opción está deshabilitada de forma predeterminada.

- Seleccione los dispositivos en los que desee instalar la aplicación:
  - **Instalar en todos los dispositivos**

    La aplicación se instalará incluso en dispositivos administrados por otros Servidores de administración.

    Esta opción está seleccionada de manera predeterminada. Si solo tiene un Servidor de administración en la red, no es necesario que cambie esta opción.

  - **Instalar solo en dispositivos administrados a través de este Servidor de administración**

    La aplicación se instalará solo en los dispositivos administrados por este Servidor de administración. Seleccione esta opción si tiene más de un Servidor de administración en su red y desea evitar conflictos entre ellos.

- Indique si los dispositivos deberán moverse a un grupo de administración después de la instalación:
  - **No mover los dispositivos**

    Los dispositivos se mantendrán en los grupos en los que se encuentren. Los dispositivos que no pertenezcan a ningún grupo quedarán sin asignar.

  - **Mover los dispositivos no asignados a este grupo (no se puede seleccionar más de un grupo)**

    Los dispositivos se moverán al grupo de administración que seleccione.

Tenga presente que la opción **No mover los dispositivos** está seleccionada de manera predeterminada. Es posible que quiera mover los dispositivos manualmente por seguridad.

7. En este paso del asistente, indique si los dispositivos deberán reiniciarse durante la instalación de las aplicaciones:

- **No reiniciar el dispositivo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

- **Reiniciar el dispositivo**

  Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

  Esta opción está seleccionada de forma predeterminada.

  - **Repetir solicitud cada (min)**

    Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

    Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

    Si no habilita esta opción, la solicitud se mostrará una sola vez.

  - **Reiniciar después de (min)**

    Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

    Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de aplicaciones en sesiones bloqueadas**

Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

Esta opción está deshabilitada de forma predeterminada.

8. De ser necesario, en el paso **Seleccione las cuentas con las que se accederá a los dispositivos**, agregue las cuentas que se utilizarán para iniciar la tarea *Instalar aplicación de forma remota*:

- **No se necesita una cuenta (el Agente de red está instalado)**

  Si selecciona esta opción, no necesitará especificar la cuenta con la que se ejecutará el instalador de la aplicación. Para ejecutar la tarea, se usará la cuenta con la que se haya iniciado el servicio del Servidor de administración.

  Esta opción no está disponible si el Agente de red no se instaló en los dispositivos cliente.

- **Se necesita una cuenta (no se utiliza el Agente de red)**

  Seleccione esta opción si el Agente de red no está instalado en los dispositivos a los que asigna la tarea de instalación remota. En este caso, puede especificar una cuenta de usuario o un certificado SSH para instalar la aplicación.

  - **Cuenta local**. Si se selecciona esta opción, especifique la cuenta bajo la que se ejecutará el instalador de aplicación. Haga clic en el botón **Agregar**, seleccione **Cuenta local** y, a continuación, especifique las credenciales de la cuenta de usuario.

    Puede especificar varias cuentas de usuario si, por ejemplo, ninguna de ellas tiene todos los derechos requeridos en todos los dispositivos a los que asigne esta tarea. En este caso, todas las cuentas añadidas se utilizan para ejecutar la tarea, en orden consecutivo de arriba abajo.

  - **Certificado de SSH**. Si desea instalar una aplicación en un dispositivo cliente basado en Linux, puede especificar un certificado SSH en lugar de una cuenta de usuario. Haga clic en el botón **Agregar**, seleccione **Certificado de SSH** y, a continuación, especifique las claves pública y privada del certificado.

    Para generar una clave privada, puede utilizar la utilidad ssh-keygen. Tenga en cuenta que Kaspersky Security Center espera que la clave privada esté en formato PEM, pero, de manera predeterminada, la utilidad ssh-keygen genera claves SSH en formato OPENSSH. Kaspersky Security Center no admite el formato OPENSSH. Para crear una clave privada en el formato PEM admitido, agregue la opción -m PEM en el comando ssh-keygen. Por ejemplo:

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "<correo electrónico del usuario>"
    ```

9. En el paso **Finalizar la creación de la tarea**, haga clic en el botón **Finalizar** para crear la tarea y cerrar el asistente.

   Si habilitó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abrirá la ventana de configuración de la tarea. Utilice esta ventana para, de ser necesario, revisar y modificar los ajustes de la tarea o programar su ejecución.

10. En la lista de tareas, seleccione la tarea creada y haga clic en **Iniciar**.

    Como alternativa, puede esperar a que ocurra el inicio programado definido en los ajustes de la tarea.

Cuando se completa la tarea de instalación remota, la aplicación seleccionada se instala en los dispositivos especificados.

## Instalar una aplicación mediante las directivas de grupo de Active Directory

Si quiere instalar una aplicación de Kaspersky en sus dispositivos administrados a través de Kaspersky Security Center, puede hacerlo mediante directivas de grupo de Active Directory.

Para instalar una aplicación utilizando directivas de grupo de Active Directory, el paquete de instalación de la misma debe incluir el Agente de red.

*Para instalar una aplicación mediante las directivas de grupo de Active Directory:*

1. Ejecute el Asistente de despliegue de la protección. Siga las instrucciones del asistente.

2. En la página **Configuración de la tarea de instalación remota** del Asistente de despliegue de la protección, seleccione la opción **Asignar la instalación del paquete en las directivas de grupo de Active Directory**.

3. En la página **Seleccione las cuentas con las que se accederá a los dispositivos**, seleccione la opción **Se necesita una cuenta (no se utiliza el Agente de red)**.

4. Agregue la cuenta con privilegios de administrador en el dispositivo donde está instalado Kaspersky Security Center o la cuenta incluida en el grupo de dominios Propietarios del creador de directivas de grupo.

5. Asigne los permisos necesarios a la cuenta seleccionada:

    a. Vaya a **Panel de control** → **Herramientas administrativas** y abra **Administración de directivas de grupo**.

    b. Haga clic en el nodo del dominio pertinente.

    c. Haga clic en la sección **Delegación**.

    d. En la lista desplegable **Permiso**, seleccione **Vincular objetos de directiva de grupo**.

    e. Haga clic en **Agregar**.

    f. En la ventana **Seleccionar usuario, equipo o grupo** que se abre, seleccione la cuenta pertinente.

    g. Haga clic en **Aceptar** para cerrar la ventana **Seleccionar usuario, equipo o grupo**.

    h. En la lista **Grupos y usuarios**, seleccione la cuenta que acaba de agregar y, luego, haga clic en **Avanzado** → **Avanzado**.

    i. En la lista **Entradas de permiso**, haga doble clic en la cuenta que acaba de agregar.

    j. Otorgue los siguientes permisos:

    - **Crear objetos de grupo**
    - **Eliminar objetos de grupo**
    - **Crear objetos de contenedor de directivas de grupo**
    - **Eliminar objetos de contenedor de directivas de grupo**

    k. Haga clic en **Aceptar** para guardar los cambios.

6. Siga las instrucciones del asistente para configurar las demás opciones.

7. Ejecute de forma manual la tarea de instalación remota creada o espere a que se inicie según la programación.

Se inicia la siguiente secuencia de instalación remota:

1. Cuando la tarea está en ejecución, en cada dominio que incluya cualquier dispositivo cliente del grupo especificado se crean los siguientes objetos:

    - Un objeto de directiva de grupo (GPO) bajo el nombre **Kaspersky_AK{GUID}**.
    - Un grupo de seguridad que corresponde al GPO. Este grupo de seguridad incluye dispositivos cliente cubiertos por la tarea. El contenido del grupo de seguridad define el alcance del GPO.

2. Kaspersky Security Center instala las aplicaciones de Kaspersky seleccionadas en los dispositivos cliente directamente desde la carpeta KLSHARE (la carpeta compartida en red de la aplicación). En la carpeta de instalación de Kaspersky Security Center, se creará una subcarpeta auxiliar anidada que contendrá el archivo .msi de la aplicación que se instalará.

3. Los dispositivos que sume al alcance de la tarea se agregarán al grupo de seguridad cuando la tarea se ejecute nuevamente. Si la opción **Ejecutar tareas no realizadas** está seleccionada en la programación de tareas, los dispositivos se agregarán de inmediato al grupo de seguridad.

4. Los dispositivos que elimine del alcance de la tarea se quitarán del grupo de seguridad cuando la tarea se ejecute nuevamente.

5. Cuando una tarea se elimina de Active Directory, también se eliminan el GPO, el enlace al GPO y el grupo de seguridad correspondiente.

Si desea aplicar otro esquema de instalación mediante Active Directory, puede configurar los parámetros requeridos manualmente. Por ejemplo, esto puede ser necesario en los siguientes casos:

- Cuando el administrador de la protección antivirus no tiene derechos para hacer cambios en Active Directory de ciertos dominios.
- Cuando el paquete de instalación original debe almacenarse en un recurso de red distinto.
- Cuando resulta necesario vincular un GPO con determinadas unidades de Active Directory.

Existen siguientes opciones para usar un esquema de instalación alternativa a través Active Directory:

- Si la instalación se realizará directamente desde la carpeta compartida de Kaspersky Security Center, en las propiedades del GPO debe especificar el archivo .msi situado en la subcarpeta exec de la carpeta del paquete de instalación para la aplicación requerida.
- Si el paquete de instalación tiene que ubicarse en otro recurso de red, debe copiar en él todo el contenido de la carpeta exec porque, además del archivo con la extensión .msi, la carpeta contiene los archivos de configuración generados cuando se creó el paquete. Para instalar la clave de licencia junto con la aplicación, copie también el archivo de clave a esta carpeta.

## Instalar aplicaciones en los Servidores de administración secundarios

*Para instalar una aplicación en Servidores de administración secundarios:*

1. Establezca conexión con el Servidor de administración que controla los servidores de administración secundarios pertinentes.

2. Asegúrese de que el paquete de instalación que corresponde a la aplicación que se está instalando esté disponible en cada uno de los Servidores de administración secundarios seleccionados. Si no puede encontrar el paquete de instalación en ninguno de los servidores secundarios, distribúyalo. Para este propósito, cree una tarea con el tipo de tarea **Distribuir paquete de instalación**.

3. Crear una tarea para la instalación de una aplicación remota en Servidores de administración secundarios. Seleccione el tipo de actividad de **Instalar aplicación en el Servidor de administración secundario de forma remota**.

   El Asistente para crear nueva tarea creará la tarea para instalar de manera remota, en servidores de administración secundarios específicos, la aplicación seleccionada en el asistente.

4. Ejecute la tarea manualmente o espere a que se inicie según la programación configurada para la tarea.

Cuando se completa la tarea de instalación remota, la aplicación seleccionada se instala en los Servidores de administración secundarios.

# Definir ajustes para instalaciones remotas en dispositivos Unix

Si va a utilizar una tarea de instalación remota para instalar una aplicación en un dispositivo Unix, puede definir ajustes específicos para Unix en la configuración de esa tarea. Una vez que cree la tarea, encontrará esos ajustes en las propiedades de la misma.

*Para definir ajustes específicos para Unix en una tarea de instalación remota:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en el nombre de la tarea de instalación remota que contendrá los ajustes específicos para Unix.

   Se abrirá la ventana de propiedades de la tarea.
3. Vaya a **Configuración de la aplicación** → **Ajustes específicos de Unix**.
4. Configure los siguientes ajustes:

   - **Definir una contraseña para la cuenta root (solo para despliegues a través de SSH)**

     Si el comando `sudo` no se puede utilizar en el dispositivo de destino sin especificar la contraseña, seleccione esta opción y luego especifique la contraseña para la cuenta root. Kaspersky Security Center transmite la contraseña de forma cifrada al dispositivo de destino, descifra la contraseña y, a continuación, inicia el procedimiento de instalación en nombre de la cuenta raíz con la contraseña especificada.

     Kaspersky Security Center no utiliza la cuenta ni la contraseña especificada para crear una conexión SSH.

   - **Especificar la ruta a una carpeta temporal con permisos de ejecución en el dispositivo de destino (solo para despliegues a través de SSH)**

     Si el directorio /tmp del dispositivo de destino no tiene permiso de ejecución, seleccione esta opción y, a continuación, especifique la ruta a un directorio que sí tenga permiso de ejecución. Kaspersky Security Center utiliza el directorio especificado como directorio temporal para el acceso a través de SSH. La aplicación pondrá el paquete de instalación en este directorio e iniciará el procedimiento de instalación.
5. Haga clic en el botón **Guardar**.

Se guardan los ajustes especificados en la tarea.

# Iniciar y detener aplicaciones de Kaspersky

Puede usar la tarea *Iniciar o detener aplicación* para iniciar y detener aplicaciones de Kaspersky en los dispositivos administrados.

*Para crear la tarea Iniciar o detener aplicación:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
3. En la lista desplegable **Aplicación**, seleccione la aplicación para la que desea crear la tarea.

   Las aplicaciones de Kaspersky aparecen en la lista si ya ha agregado complementos web de administración para ellas.
4. En la lista **Tipo de tarea**, seleccione la tarea **Activación de la aplicación**.
5. En el campo **Nombre de la tarea**, ingrese el nombre de la tarea nueva.

   El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).
6. Seleccione los dispositivos a los que se asignará la tarea.
7. En la ventana **Aplicaciones**, haga lo siguiente:
   - Marque las casillas junto a los nombres de las aplicaciones para las que desee crear la tarea.
   - Seleccione la opción **Iniciar la aplicación** o **Detener la aplicación**.
8. Si desea modificar la configuración predeterminada de la tarea, active la opción **Abrir los detalles de la tarea cuando se complete la creación** en el paso **Finalizar la creación de la tarea**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.
9. Haga clic en el botón **Finalizar**.

   Se crea la tarea y se la agrega a la lista de tareas.
10. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.
11. En la ventana de propiedades de la tarea, defina los ajustes generales de la tarea que se adapten a sus necesidades y luego guárdelos.

La tarea queda creada y configurada.

Para ejecutar la tarea, selecciónela en la lista de tareas y haga clic en el botón **Iniciar**.

# Administración de dispositivos móviles

La administración de protección del dispositivo móvil a través de Kaspersky Security Center se realiza usando la función Administración de dispositivos móviles, que exige una licencia especializada. Habilite y configure la característica Administración de dispositivos móviles si planea administrar dispositivos móviles que pertenezcan a los empleados de su organización.

Podrá usar las funciones de Administración de dispositivos móviles para gestionar los dispositivos Android del personal. La aplicación móvil Kaspersky Endpoint Security para Android instalada en los dispositivos proporciona la protección. Esta aplicación móvil garantiza la protección de los dispositivos móviles contra amenazas web, virus y otros programas que representan amenazas. Para una administración centralizada a través de Kaspersky Security Center Web Console, debe instalar los siguientes complementos de administración web en el dispositivo donde está instalado Kaspersky Security Center Web Console:

- Complemento de Kaspersky Security for Mobile
- Complemento de Kaspersky Endpoint Security para Android

Para obtener información sobre el despliegue de la protección y la administración de dispositivos móviles, consulte la Ayuda de Kaspersky Security para dispositivos móviles.

## Modificar la configuración de Administración de dispositivos móviles en Kaspersky Security Center Web Console

*Para modificar la configuración de administración de dispositivos móviles:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, seleccione **Puertos adicionales**.

3. Modifique la configuración relevante:

- **Abrir puerto para dispositivos móviles**

  Si este conmutador está activado, el puerto para dispositivos móviles se abrirá en el Servidor de administración.

  Puede utilizar el puerto para dispositivos móviles solo si se encuentra instalado el componente de administración de dispositivos móviles.

  Si se desactiva el conmutador, no se utilizará el puerto para dispositivos móviles en el Servidor de administración.

  Esta opción está desactivada de manera predeterminada.

- **Puerto para la sincronización de dispositivos móviles**

  Número del puerto que se utiliza para conectar dispositivos móviles al Servidor de administración. El número de puerto predeterminado es 13292.

  El sistema decimal se usa para los registros.

- **Puerto para la activación de dispositivos móviles**

  Puerto que Kaspersky Endpoint Security para Android usará para conectarse con los servidores de activación de Kaspersky.

  El número de puerto predeterminado es 17100.

4. Haga clic en el botón **Guardar**.

Los dispositivos móviles pueden conectarse ahora al Servidor de administración.

# Reemplazo de aplicaciones de seguridad de terceros

La Instalación de aplicaciones de seguridad de Kaspersky a través de Kaspersky Security Center puede requerir la eliminación del software de terceros incompatible con la aplicación instalada. Kaspersky Security Center proporciona varias formas de eliminar las aplicaciones de terceros.

## Eliminar aplicaciones incompatibles utilizando el instalador

Esta opción está disponible solo en la Consola de administración basada en Microsoft Management Console.

El método del programa de instalación de eliminar aplicaciones incompatibles es compatible con varios tipos de instalación. Antes de la instalación de la aplicación de seguridad, todas las aplicaciones incompatibles se eliminan automáticamente si la ventana de propiedades del paquete de instalación de esta aplicación de seguridad (sección **Aplicaciones incompatibles**) tiene la opción **Desinstalar aplicaciones incompatibles automáticamente** seleccionada.

### Eliminar aplicaciones incompatibles al configurar la instalación remota de una aplicación

Cuando esté configurando la instalación remota de una aplicación de seguridad, puede habilitar la opción **Desinstalar aplicaciones incompatibles automáticamente**. En la Consola de administración basada en Microsoft Management Console (MMC), esta opción está disponible en el Asistente de instalación remota. En Kaspersky Security Center Web Console, puede encontrar esta opción en el Asistente de despliegue de la protección. Cuando esta opción se habilita, Kaspersky Security Center elimina la aplicación incompatible antes de instalar una aplicación de seguridad en un dispositivo administrado.

Instrucciones:

- Consola de administración: Eliminación de aplicaciones mediante el Asistente de instalación remota
- Kaspersky Security Center Web Console: Eliminar aplicaciones incompatibles antes de la instalación

### Eliminar aplicaciones incompatibles a través de una tarea dedicada

Para eliminar aplicaciones incompatibles, use la tarea **Desinstalar aplicación de forma remota**. Esta tarea se debe ejecutar en los dispositivos antes que la tarea para instalar la aplicación de seguridad. Por ejemplo, en la tarea de instalación, puede seleccionar **Al completarse otra tarea** con el tipo de programación, en el que la otra tarea es **Desinstalar aplicación de forma remota**.

Este método de desinstalación es útil cuando el instalador de la aplicación de seguridad no puede eliminar correctamente una aplicación incompatible.

Instrucciones para la Consola de administración: Crear una tarea.

# Descubrimiento de dispositivos conectados a la red

Esta sección describe la búsqueda y la detección de dispositivos conectados a una red.

Kaspersky Security Center le permite encontrar dispositivos según criterios especificados. Los resultados de estas búsquedas se pueden guardar en un archivo de texto.

La función de búsqueda y la detección permite encontrar los siguientes dispositivos:

- Dispositivos administrados en grupos de administración del Servidor de administración de Kaspersky Security Center y sus Servidores de administración secundarios.
- Dispositivos no asignados administrados por el Servidor de administración de Kaspersky Security Center y sus Servidores de administración secundarios.

# Escenario: Descubrir dispositivos conectados a la red

Antes de instalar las aplicaciones de seguridad, es necesario llevar a cabo un descubrimiento de dispositivos. El Servidor de administración recibe información sobre los dispositivos descubiertos y le permite administrar los dispositivos a través de directivas. Se necesitan sondeos de red regulares para actualizar la lista de dispositivos disponibles en la red.

Antes de iniciar el sondeo de red, asegúrese de que el protocolo SMB esté habilitado. De lo contrario, Kaspersky Security Center no puede detectar dispositivos en la red sondeada. Para habilitar el protocolo SMB, siga las instrucciones para su sistema operativo.

La detección de dispositivos en red se realiza en las siguientes etapas:

1. **Descubrir dispositivos**

   Utilice el Asistente de inicio rápido para realizar un descubrimiento de dispositivos inicial y detectar computadoras, tablets, teléfonos móviles y otros dispositivos conectados a la red. También puede realizar el descubrimiento de dispositivos manualmente.

2. **Configurar sondeos programados**

   Decida qué tipo(s) de sondeo desea utilizar regularmente. Habilite los tipos deseados y configure la programación del sondeo. Puede referirse a las recomendaciones para la frecuencia de sondeo de red.

3. **Configurar reglas para que los dispositivos descubiertos se agreguen a grupos de administración (opcional)**

   Si aparecen nuevos dispositivos de la red, que se detectan durante las encuestas regulares y se incluyen automáticamente en el grupo **Dispositivos no asignados**. Puede configurar reglas de movimiento de dispositivos para automatizar la asignación de dispositivos al grupo **Dispositivos administrados**. También puede configurar las reglas de retención.

   Si omite el paso 3, los dispositivos recién descubiertos se asignan al grupo **Dispositivos no asignados**. Si lo desea, puede mover estos dispositivos manualmente al grupo **Dispositivos administrados**. Si mueve los dispositivos manualmente al grupo **Dispositivos administrados**, puede analizar la información sobre cada dispositivo y decidir si desea moverlo a un grupo de administración, y, de ser así, a qué grupo exacto.

## Resultados

Completar las etapas anteriores tiene los siguientes resultados:

- El Servidor de administración de Kaspersky Security Center detecta los dispositivos que están en la red y le proporciona información sobre ellos.
- Los sondeos futuros se configuran y funcionan de acuerdo con el calendario programado.
- Los dispositivos recién descubiertos se arreglan según las reglas configuradas. (O, si no se configura ninguna regla, los dispositivos se quedan en el grupo **Dispositivos no asignados**).

# Descubrimiento de dispositivos

Esta sección describe los tipos de descubrimiento de dispositivos disponibles en Kaspersky Security Center y proporciona información sobre cada tipo.

El Servidor de administración recibe información sobre la estructura de la red y los dispositivos en esta red a través de un sondeo regular. La información se registra en la base de datos del Servidor de administración. El Servidor de administración puede utilizar los siguientes tipos de sondeo:

- **Sondeo de la red de Windows**. El Servidor de administración puede realizar dos tipos de sondeos de red de Windows: rápida y completa. Cuando se realiza un sondeo rápido, el Servidor de administración solo recupera información de la lista de nombres NetBIOS correspondientes a los dispositivos de todos los dominios y grupos de trabajo de la red. Durante un sondeo completo, se solicita más información desde cada dispositivo cliente, como el nombre del sistema operativo, la dirección IP, el nombre DNS y el nombre NetBIOS. De forma predeterminada, tanto el sondeo rápido como el sondeo completo están habilitados. El sondeo de la red de Windows puede no detectar dispositivos, por ejemplo, si los puertos UDP 137, UDP 138, TCP 139 están cerrados en el enrutador o por el firewall.

- **Sondeo del controlador de dominio**. El Servidor de administración o un punto de distribución recupera información sobre la estructura del dominio y sobre los nombres DNS de los dispositivos incluidos en el dominio. Por defecto, este tipo de sondeo está habilitado. Recomendamos que utilice el sondeo de controlador de dominio si todos los dispositivos en red son miembros de un dominio. Si algunos de los dispositivos en red no están incluidos en el dominio, estos dispositivos no podrán ser descubiertos mediante el sondeo de controlador de dominio.

- **Sondeo de intervalos IP**. El Servidor de administración utiliza paquetes ICMP o el protocolo NBNS para sondear los intervalos IP especificados y recopilar una serie de datos completa sobre los dispositivos incluidos en esos intervalos. Este tipo de sondeo está deshabilitado de manera predeterminada. No se recomienda usar este tipo de sondeo si ya realiza sondeos de la red de Windows o de Active Directory.

- **Sondeo de Zeroconf**. Un punto de distribución que sondea la red IPv6 mediante el uso de una red de configuración cero (también denominada *Zeroconf*). Este tipo de sondeo está deshabilitado de manera predeterminada. Puede usar el sondeo de Zeroconf si el punto de distribución ejecuta Linux.

Si configura y habilita reglas de movimiento de dispositivos, los dispositivos recién descubiertos se incluirán de forma automática en el grupo **Dispositivos administrados**. Si no se han habilitado reglas de movimiento, los dispositivos recién descubiertos se incluyen automáticamente en el grupo **Dispositivos no asignados**.

Puede modificar la configuración de descubrimiento de dispositivos para cada tipo. Por ejemplo, puede cambiar la frecuencia con la que se realizan los sondeos o definir si el sondeo del dominio alcanzará a todo el bosque o estará limitado a un dominio específico.

Antes de iniciar el sondeo de red, asegúrese de que el protocolo SMB esté habilitado. De lo contrario, Kaspersky Security Center no puede detectar dispositivos en la red sondeada. Para habilitar el protocolo SMB, siga las instrucciones para su sistema operativo.

# Sondeo de la red de Windows

## Acerca del sondeo de la red de Windows

Cuando se realiza un sondeo rápido, el Servidor de administración solo recupera información de la lista de nombres NetBIOS correspondientes a los dispositivos de todos los dominios y grupos de trabajo de la red. Cuando se realiza un sondeo completo, se solicita la siguiente información a cada dispositivo cliente:

- Nombre del sistema operativo
- Dirección IP
- Nombre DNS
- Nombre NetBIOS

Para realizar un sondeo rápido o completo, se deben cumplir los siguientes requisitos:

- Los puertos UDP 137/138, TCP 139, UDP 445, TCP 445 deben estar disponibles en la red.
- El protocolo SMB está activado.
- Se debe utilizar el servicio Explorador de equipos de Microsoft y el equipo del navegador principal debe estar habilitado en el Servidor de administración.
- Se debe utilizar el servicio Explorador de equipos de Microsoft y el equipo explorador principal debe estar habilitado en esta cantidad de dispositivos cliente:
  - al menos un dispositivo si no hay más de 32 dispositivos conectados a la red;
  - al menos un dispositivo por cada 32 dispositivos conectados a la red.

Para realizar un sondeo completo, primero debe haberse realizado al menos un sondeo rápido.

## Cómo ver y modificar la configuración del sondeo de la red de Windows

*Para modificar las propiedades del sondeo de la red de Windows:*

1. En el menú principal, vaya a **Descubrimiento y despliegue** → **Descubrimiento** → **Dominios de Windows**.
2. Haga clic en el botón **Propiedades**.

   Se abrirá la ventana de propiedades del dominio de Windows.
3. Utilizando el interruptor **Habilitar el sondeo de la red de Windows**, habilite o deshabilite el sondeo de la red de Windows.

4. Configurar la programación del sondeo. De forma predeterminada, el sondeo rápido se ejecuta cada 15 minutos y el sondeo completo se ejecuta cada 60 minutos.

   Opciones de programación para el sondeo:

   - **Cada N días**

     Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la fecha y hora indicadas. Cada sondeo estará separado del anterior por el número de días que indique.

     De forma predeterminada, se realizará un sondeo todos los días, a partir de la fecha y hora actuales del sistema.

   - **Cada N minutos**

     Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la hora indicada. Cada sondeo estará separado del anterior por el número de minutos que indique.

   - **Por días de la semana**

     Se realizará un sondeo en forma periódica, a intervalos regulares, en el día de la semana y a la hora que indique.

   - **Cada mes en los días especificados de semanas seleccionadas**

     Se realizará un sondeo en forma periódica, a intervalos regulares, en los días del mes y a la hora que indique.

   - **Ejecutar tareas no realizadas**

     Si el Servidor de administración está apagado o no está disponible durante la hora programada para el sondeo, el Servidor de administración puede iniciar el sondeo inmediatamente después de encenderlo o esperar la próxima vez que se programe el sondeo.

     Si esta opción está habilitada, el Servidor de administración inicia el sondeo inmediatamente después de que se enciende.

     Si esta opción está desactivada, el Servidor de administración espera la próxima vez que se programe el sondeo.

     Esta opción está deshabilitada de forma predeterminada.

5. Guardar las propiedades del sondeo de la red de Windows.

Las propiedades se guardan y se aplican a todos los dominios y grupos de trabajo de Windows descubiertos.

## Ejecutando la encuesta manualmente

*Para ejecutar la encuesta de inmediato,*

Haga clic en **Iniciar sondeo rápido** o en **Iniciar sondeo completo**.

Cuando se completa el sondeo, puede ver la lista de dispositivos descubiertos en la página **Dominios de Windows** al seleccionar la casilla de verificación junto a un nombre de dominio y luego hacer clic en el botón **Dispositivos**.

## Sondeo de intervalos IP

Inicialmente, Kaspersky Security Center obtiene rangos de IP para el sondeo desde la configuración de red del dispositivo en el que está instalado. Si la dirección del dispositivo es 192.168.0.1 y la máscara de subred es 255.255.255.0, Kaspersky Security Center incluye automáticamente la red 192.168.0.0/24 en la lista de direcciones del sondeo. Kaspersky Security Center sondea todas las direcciones desde 192.168.0.1 hasta 192.168.0.254.

Para todos los hosts basados en Linux dentro de un controlador de dominio de Microsoft Active Directory o Samba, especifique el `netbios name` y los parámetros del `workgroup` en el archivo `/etc/samba/smb.conf`. Si no lo hace, es posible que los resultados del sondeo contengan hosts duplicados.

Para sondear un intervalo IP, Kaspersky Security Center puede emplear dos estrategias: realizar consultas DNS inversas o utilizar el protocolo NBNS.

- **Consultas DNS inversas**

  Kaspersky Security Center lleva a cabo una operación de resolución inversa para intentar determinar, mediante consultas DNS estándar, el nombre DNS correspondiente a cada dirección IP del intervalo especificado. Si esta operación tiene éxito, el servidor envía al nombre recibido un `ICMP ECHO REQUEST` (el mismo tipo de solicitud que se utiliza en el comando ping). Si el dispositivo responde, la información se agrega a la base de datos de Kaspersky Security Center. La resolución de nombres inversa es necesaria para excluir dispositivos de red que pueden tener dirección IP, pero que no son computadoras (por ejemplo, impresoras y routers).

  Para que este método de sondeo funcione, debe haber un servicio de DNS local correctamente configurado. El servicio debe tener una zona de búsqueda inversa. En las redes donde se utiliza Active Directory, esta zona se mantiene automáticamente. Pero en estas redes, el sondeo de subred IP no proporciona más información que el sondeo de Active Directory. Además, quienes administran una red pequeña rara vez configuran la zona de búsqueda inversa, pues no todos los servicios de red la necesitan para operar. Por estos motivos, el sondeo de subredes IP está deshabilitado de forma predeterminada.

- **Protocolo NBNS**

  Si algo impide llevar a cabo una resolución de nombres inversa en la red, para sondear los intervalos de direcciones IP, Kaspersky Security Center usará el protocolo NBNS. Si Kaspersky Security Center realiza una solicitud a una dirección IP y obtiene un nombre NetBIOS como respuesta, agregará información sobre el dispositivo correspondiente a su base de datos.

Antes de iniciar el sondeo de red, asegúrese de que el protocolo SMB esté habilitado. De lo contrario, Kaspersky Security Center no puede detectar dispositivos en la red sondeada. Para habilitar el protocolo SMB, siga las instrucciones para su sistema operativo.

### Cómo ver y modificar la configuración del sondeo de intervalos IP

*Para ver y modificar las propiedades del sondeo de intervalos IP:*

1. En el menú principal, vaya a **Descubrimiento y despliegue** → **Descubrimiento** → **Intervalos IP**.
2. Haga clic en el botón **Propiedades**.

   Se abre la ventana de propiedades de sondeo de IP.

3. Utilizando el interruptor **Permitir sondeo**, habilite o deshabilite el sondeo de intervalos IP.

4. Configurar la programación del sondeo. De forma predeterminada, el sondeo de intervalos IP se ejecuta cada 420 minutos (7 horas).

   Al definir la frecuencia de sondeo, asegúrese de usar un valor que no supere el del parámetro Vigencia de la dirección IP. Si la función de sondeo no verifica que una dirección IP se encuentra activa durante el tiempo de vigencia de las direcciones IP, la dirección se elimina automáticamente de los resultados del sondeo. Los resultados de los sondeos tienen una vida útil por defecto de veinticuatro horas; esto se debe a que las direcciones IP dinámicas (las que se asignan mediante el protocolo de configuración dinámica de hosts, DHCP) cambian cada veinticuatro horas.

   Opciones de programación para el sondeo:

   - **Cada N días**

     Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la fecha y hora indicadas. Cada sondeo estará separado del anterior por el número de días que indique.

     De forma predeterminada, se realizará un sondeo todos los días, a partir de la fecha y hora actuales del sistema.

   - **Cada N minutos**

     Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la hora indicada. Cada sondeo estará separado del anterior por el número de minutos que indique.

   - **Por días de la semana**

     Se realizará un sondeo en forma periódica, a intervalos regulares, en el día de la semana y a la hora que indique.

   - **Cada mes en los días especificados de semanas seleccionadas**

     Se realizará un sondeo en forma periódica, a intervalos regulares, en los días del mes y a la hora que indique.

   - **Ejecutar tareas no realizadas**

     Si el Servidor de administración está apagado o no está disponible durante la hora programada para el sondeo, el Servidor de administración puede iniciar el sondeo inmediatamente después de encenderlo o esperar la próxima vez que se programe el sondeo.

     Si esta opción está habilitada, el Servidor de administración inicia el sondeo inmediatamente después de que se enciende.

     Si esta opción está desactivada, el Servidor de administración espera la próxima vez que se programe el sondeo.

     Esta opción está deshabilitada de forma predeterminada.

5. Haga clic en el botón **Guardar**.

Las propiedades se guardan y se aplican a todos los intervalos IP.

### Ejecutando la encuesta manualmente

*Para ejecutar la encuesta de inmediato,*

haga clic en **Iniciar sondeo**.

## Agregar y modificar un intervalo IP

Inicialmente, Kaspersky Security Center obtiene rangos de IP para el sondeo desde la configuración de red del dispositivo en el que está instalado. Si la dirección del dispositivo es 192.168.0.1 y la máscara de subred es 255.255.255.0, Kaspersky Security Center incluye automáticamente la red 192.168.0.0/24 en la lista de direcciones del sondeo. Kaspersky Security Center sondea todas las direcciones desde 192.168.0.1 hasta 192.168.0.254. Puede modificar los intervalos IP definidos automáticamente o agregar intervalos IP personalizados.

Puede crear un rango solo para direcciones IPv4. Si habilita el Sondeo de Zeroconf, Kaspersky Security Center sondea toda la red.

*Para agregar un nuevo intervalo IP:*

1. En el menú principal, vaya a **Descubrimiento y despliegue** → **Descubrimiento** → **Intervalos IP**.
2. Para agregar un nuevo intervalo IP, haga clic en el botón **Agregar**.
3. En la ventana que se abre, defina los siguientes ajustes:
   - **Nombre del intervalo IP**

     Nombre que se le dará al intervalo IP. El nombre puede ser el intervalo en sí mismo (por ejemplo, "192.168.0.0/24").
   - **Intervalo IP o dirección y máscara de subred**

     Establezca el intervalo IP especificando las direcciones IP iniciales y finales o la dirección de subred y la máscara de subred. También puede seleccionar uno de los rangos IP existentes haciendo clic en el botón **Examinar**.
   - **Vigencia de la dirección IP (h)**

     Al configurar este ajuste, asegúrese de que el valor supere el intervalo de sondeo establecido en la programación de sondeos. Si la función de sondeo no verifica que una dirección IP se encuentra activa durante el tiempo de vigencia de las direcciones IP, la dirección se elimina automáticamente de los resultados del sondeo. Los resultados de los sondeos tienen una vida útil por defecto de veinticuatro horas; esto se debe a que las direcciones IP dinámicas (las que se asignan mediante el protocolo de configuración dinámica de hosts, DHCP) cambian cada veinticuatro horas.
4. Seleccione **Habilitar el sondeo de intervalos IP** si desea sondear la subred o el intervalo que agregó. De lo contrario, la subred o el intervalo que ha añadido no se sondearán.
5. Haga clic en el botón **Guardar**.

El nuevo intervalo IP se agrega a la lista de intervalos IP.

Puede ejecutar el sondeo de cada rango IP por separado usando el botón **Iniciar sondeo**. Cuando se complete el sondeo, haga clic en el botón **Dispositivos** para ver la lista de dispositivos descubiertos. De forma predeterminada, los resultados del sondeo serán válidos por veinticuatro horas (el mismo tiempo por el que se considera vigente una dirección IP).

*Para agregar una subred a un rango IP existente:*

1. En el menú principal, vaya a **Descubrimiento y despliegue** → **Descubrimiento** → **Intervalos IP**.
2. Haga clic en el nombre del rango IP al que desea agregar una subred.
3. En la ventana que se abre, haga clic en el botón **Agregar**.
4. Especifique una subred usando su dirección y máscara o usando la primera y la última dirección IP en el intervalo IP. O, agregue una subred existente haciendo clic en el botón **Examinar**.
5. Haga clic en el botón **Guardar**.

   La nueva subred se agrega al rango IP.
6. Haga clic en el botón **Guardar**.

La nueva configuración del rango IP se guarda.

Puede agregar todas las subredes que necesite. Los intervalos IP con nombre no se pueden superponer, pero no existe tal restricción para las subredes sin nombre contenidas en un intervalo IP. Puede habilitar y deshabilitar el sondeo de forma independiente para cada rango IP.

## Sondeo con Zeroconf

Este tipo de sondeo solo es compatible con los puntos de distribución basados en Linux.

Un punto de distribución puede sondear las redes que tienen dispositivos con direcciones IPv6. En este caso, no se especifican los rangos de IP y el punto de distribución sondea toda la red mediante el uso de una red de configuración cero (denominada *Zeroconf*). Para empezar a usar Zeroconf, debe instalar la utilidad avahi-browse en el punto de distribución.

*Para habilitar el sondeo de red IPv6, haga lo siguiente:*

1. En el menú principal, vaya a **Descubrimiento y despliegue** → **Descubrimiento** → **Intervalos IP**.
2. Haga clic en el botón **Propiedades**.
3. En la ventana que se abre, active el botón de alternancia **Usar Zeroconf para el sondeo de redes IPv6**.

Después de esto, el punto de distribución empieza a sondear su red. En este caso, se ignoran los rangos de IP especificados.

# Sondeo del controlador de dominio

Kaspersky Security Center admite el sondeo de un controlador de dominio Active Directory de Microsoft y un controlador de dominio Samba.

Kaspersky Security Center permite sondear un controlador de dominio Samba solo mediante un punto de distribución de Linux. Para un controlador de dominio Samba, se utiliza Samba 4 como controlador de dominio de Active Directory.

Cuando sondea un controlador de dominio, el Servidor de administración o un punto de distribución recupera información sobre la estructura del dominio, las cuentas de usuario, los grupos de seguridad y los nombres DNS de los dispositivos incluidos en el dominio.

Recomendamos utilizar el sondeo de controlador de dominio si todos los dispositivos en red son miembros de un dominio. Si algunos de los dispositivos en red no están incluidos en el dominio, estos dispositivos no podrán ser descubiertos mediante el sondeo de controlador de dominio.

## Requisitos previos

Antes de sondear un controlador de dominio, asegúrese de que se permitan las conexiones al controlador de dominio a través de un firewall o servidor proxy. También asegúrese de que los siguientes protocolos estén habilitados en el controlador de dominio:

- Protocolo ligero de acceso a directorios (LDAP)
- Capa de seguridad y autenticación simple (SASL)

  Este protocolo se usa si la conexión al controlador de dominio se establece mediante la autenticación SASL. El Servidor de administración y los puntos de distribución solo admiten el mecanismo DIGEST-MD5.
- Protocolo ligero de acceso a directorios a través de la capa de sockets seguros (LDAPS)

  Este protocolo se utiliza si necesita conectarse al controlador de dominio mediante una conexión cifrada.

Asegúrese de que los siguientes puertos estén disponibles en el dispositivo controlador de dominio:

- 389 para el protocolo LDAP y autenticación simple (incluido SASL)
- 636 para el protocolo LDAPS

Para todos los hosts basados en Linux dentro de un controlador de dominio Samba o Microsoft Active Directory, debe especificar los parámetros `netbios name` y `workgroup` en el archivo `/etc/samba/smb.conf`. Si no lo hace, es posible que los resultados del sondeo contengan hosts duplicados.

Si un dominio de Microsoft Active Directory contiene varios controladores de dominio, no se admite la selección de un controlador específico durante el sondeo de dominios. La conexión se establece con el primer controlador de dominio detectado. Para garantizar una autenticación adecuada con el dominio de Microsoft Active Directory, el campo Nombre alternativo del sujeto (SAN) del certificado debe incluir todas las direcciones de los controladores de dominio incluidos en este dominio, así como el nombre NetBIOS del dominio de Microsoft Active Directory.

## Sondeo de controlador de dominio mediante el Servidor de administración

Puede usar el Servidor de administración para sondear solo un controlador de dominio Active Directory de Microsoft.

*Para sondear un controlador de dominio mediante el Servidor de administración:*

1. En el menú principal, vaya a **Descubrimiento y despliegue** → **Descubrimiento** → **Controladores de dominio**.
2. Haga clic en **Configuración de sondeo**.

   Se abrirá la ventana **Configuración del sondeo de controladores de dominio**.
3. Seleccione la opción **Habilitar el sondeo de controladores de dominio**.
4. En la sección **Configuración avanzada**, especifique el alcance del sondeo:

   - **Sondear dominio actual**

     Seleccione esta opción para sondear un dominio al que pertenece Kaspersky Security Center.

   - **Sondear bosque de dominio entero**

     Seleccione esta opción para sondear un bosque de dominio al que pertenece Kaspersky Security Center.

   - **Sondear dominios específicos**

     Seleccione esta opción para sondear un dominio con la dirección y las credenciales de usuario especificadas.

5. Si es necesario, especifique la frecuencia de los sondeos. La frecuencia de sondeo predeterminada es de una hora. Los datos recibidos en un sondeo reemplazan completamente a los datos del sondeo anterior.

   Las siguientes opciones de horarios de sondeo están disponibles:

   - **Cada N días**

     Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la fecha y hora indicadas. Cada sondeo estará separado del anterior por el número de días que indique.

     De forma predeterminada, se realizará un sondeo todos los días, a partir de la fecha y hora actuales del sistema.

   - **Cada N minutos**

     Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la hora indicada. Cada sondeo estará separado del anterior por el número de minutos que indique.

   - **Por días de la semana**

     Se realizará un sondeo en forma periódica, a intervalos regulares, en el día de la semana y a la hora que indique.

   - **Cada mes en los días especificados de semanas seleccionadas**

     Se realizará un sondeo en forma periódica, a intervalos regulares, en los días del mes y a la hora que indique.

   - **Ejecutar tareas no realizadas**

     Si el Servidor de administración está apagado o no está disponible durante la hora programada para el sondeo, el Servidor de administración puede iniciar el sondeo inmediatamente después de encenderlo o esperar la próxima vez que se programe el sondeo.

     Si esta opción está habilitada, el Servidor de administración inicia el sondeo inmediatamente después de que se enciende.

     Si esta opción está desactivada, el Servidor de administración espera la próxima vez que se programe el sondeo.

     Esta opción está deshabilitada de forma predeterminada.

   Si cambia las cuentas de usuario en un grupo de seguridad del dominio, estos cambios se mostrarán en Kaspersky Security Center una hora después de sondear el controlador de dominio.

6. Haga clic en **Guardar** para aplicar los cambios.

7. Si desea realizar el sondeo inmediatamente, haga clic en el botón **Iniciar sondeo**.

## Sondeo de controlador de dominio mediante el uso de un punto de distribución

También puede sondear un controlador de dominio de Active Directory de Microsoft y un controlador de dominio Samba mediante un punto de distribución. Un dispositivo administrado basado en Windows o Linux puede actuar como punto de distribución.

Para un punto de distribución de Linux, se admite el sondeo de un controlador de dominio Microsoft Active Directory y un controlador de dominio Samba.
Para un punto de distribución de Windows, solo se admite el sondeo de un controlador de dominio de Microsoft Active Directory.
No se admite el sondeo con un punto de distribución de Mac.

*Para configurar el sondeo de controlador de dominio mediante el punto de distribución:*

1. Abra las propiedades del punto de distribución.
2. Seleccione la sección **Sondeo del controlador de dominio**.
3. Seleccione la opción **Habilitar el sondeo de controladores de dominio**.
4. Seleccione el controlador de dominio que desea sondear.

   Si utiliza un punto de distribución de Linux, en la sección **Sondear dominios específicos**, haga clic en **Agregar** y luego especifique la dirección y las credenciales de usuario del controlador de dominio.

   Si utiliza un punto de distribución de Windows, puede seleccionar una de las siguientes opciones:

   - **Sondear dominio actual**
   - **Sondear bosque de dominio entero**
   - **Sondear dominios específicos**
5. Haga clic en el botón **Establecer programación de sondeo** para especificar las opciones del programa de sondeo si es necesario.

   El sondeo comenzará según el programa especificado únicamente. El inicio manual del sondeo no está disponible.

Una vez completado el sondeo, la estructura del dominio se mostrará en la sección **Controladores de dominio**.

Si configura y habilita reglas de movimiento de dispositivos, los dispositivos recién descubiertos se incluirán de forma automática en el grupo **Dispositivos administrados**. Si no se han habilitado reglas de movimiento, los dispositivos recién descubiertos se incluyen automáticamente en el grupo **Dispositivos no asignados**.

Las cuentas de usuario descubiertas se pueden utilizar para la autenticación de dominio en Kaspersky Security Center Web Console.

# Autenticación y conexión a un controlador de dominio

## Autenticación y conexión a un controlador de dominio al sondear un dominio

Al sondear un controlador de dominio con un punto de distribución con Linux, el punto de distribución identifica el protocolo de conexión para establecer la conexión inicial con el controlador de dominio. El protocolo se usa de allí en más para todas las futuras conexiones con el controlador de dominio Cuando se establezca la conexión inicial con el controlador de dominio, puede cambiar las opciones de conexión utilizando los indicadores del Agente de red (`KLNAG_LDAP_TLS_REQCERT` y `KLNAG_LDAP_SSL_CACERT`). Puede configurar los indicadores del Agente de red con klscflag como se describe en este artículo.

La conexión inicial a un controlador de dominio se realiza de la siguiente manera:

1. Un punto de distribución con Linux intenta conectarse al controlador de dominio mediante el protocolo LDAPS.

   De forma predeterminada, la verificación del certificado no es obligatoria. Establezca el indicador `KLNAG_LDAP_TLS_REQCERT` en 1 para verificar el certificado.

   Valores posibles del indicador `KLNAG_LDAP_TLS_REQCERT`:

   - `0`: se solicita el certificado, pero si la otra parte no brinda un certificado o si la verificación del certificado genera un error, se considera que la conexión TLS se estableció correctamente (valor predeterminado).
   - `1`: se requiere una verificación estricta del certificado del servidor LDAP.

   De forma predeterminada, si no se especifica el indicador `KLNAG_LDAP_SSL_CACERT`, se usa la ruta de acceso a la entidad de certificación (CA) que brinda el sistema operativo para acceder a la cadena de certificados. Utilice el indicador `KLNAG_LDAP_SSL_CACERT` para especificar una ruta personalizada.

2. Si la conexión LDAPS falla, un punto de distribución de Linux intenta conectarse al controlador de dominio a través de una conexión TCP no cifrada mediante SASL (DIGEST-MD5).

## Configuración de indicadores

Puede usar la utilidad klscflag para configurar los indicadores.

En un punto de distribución con Linux, ejecute la línea de comandos y pase al directorio que contenga la utilidad klscflag. Por defecto, en el punto de distribución de Linux , la utilidad klscflag se encuentra en / opt / kaspersky / ksc64 / sbin.

El siguiente comando, por ejemplo, habilita la verificación de certificados:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

# Configurar un controlador de dominio Samba

Kaspersky Security Center admite un controlador de dominio de Linux que se ejecuta únicamente en Samba 4.

Un controlador de dominio Samba admite las mismas extensiones de esquema que un controlador de dominio Microsoft Active Directory. Puede habilitar la compatibilidad total de un controlador de dominio Samba con un controlador de dominio Microsoft Active Directory utilizando la extensión de esquema Samba 4. Esta acción es opcional.

Recomendamos habilitar la compatibilidad total de un controlador de dominio Samba con un controlador de dominio Microsoft Active Directory. Esto garantizará la interacción correcta entre Kaspersky Security Center y el controlador de dominio Samba.

*Para habilitar la compatibilidad total de un controlador de dominio Samba con un controlador de dominio Microsoft Active Directory:*

1. Ejecute el siguiente comando para utilizar la extensión de esquema RFC2307:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Habilite la actualización del esquema en un controlador de dominio Samba. Para ello, agregue la siguiente línea al archivo `/etc/samba/smb.conf`:

   ```
   dsdb:schema update allowed = true
   ```

   Si la actualización del esquema se completa con un error, deberá realizar una restauración completa del controlador de dominio que actúa como maestro de esquema.

Para todos los hosts basados en Linux dentro de un controlador de dominio Samba, especifique los parámetros `netbios name` y `workgroup` en el archivo `/etc/samba/smb.conf`. Si no lo hace, es posible que los resultados del sondeo contengan hosts duplicados.

## Configuración de reglas de retención para dispositivos no asignados

Una vez finalizado el sondeo de la red de Windows, los dispositivos descubiertos se colocan en subgrupos del grupo de administración "Dispositivos no asignados". Este grupo de administración se encuentra en **Descubrimiento y despliegue → Descubrimiento → Dominios de Windows**. El grupo primario es la carpeta **Dominios de Windows**. Dicha carpeta contiene grupos secundarios que llevan el nombre de los dominios y grupos de trabajo descubiertos durante el sondeo. El grupo primario también puede contener el grupo de administración de dispositivos móviles. Puede configurar las reglas de retención de dispositivos no asignados para el grupo primario y para cada uno de los grupos secundarios. Las reglas de retención no dependen de la configuración del descubrimiento de dispositivos y funcionan incluso si el descubrimiento de dispositivos está deshabilitado.

Las reglas de retención de dispositivos no afectan a los dispositivos que tienen una o más unidades cifradas con cifrado de disco completo. Dichos dispositivos no se eliminan automáticamente, solo puede hacerlo de forma manual. Si necesita eliminar un dispositivo con una unidad cifrada, primero descifre la unidad y luego elimine el dispositivo.

*Para configurar las reglas de retención para dispositivos no asignados:*

1. En el menú principal, vaya a **Descubrimiento y despliegue** → **Descubrimiento** → **Dominios de Windows**.
2. Realice una de las siguientes acciones:
   - Para configurar los ajustes del grupo primario, haga clic en el botón **Propiedades**.

     Se abrirá la ventana de propiedades del dominio de Windows.
   - Para configurar los ajustes de un grupo secundario, haga clic en su nombre.

     Se abrirá la ventana de propiedades del grupo secundario.
3. Defina los siguientes parámetros de configuración:
   - **Eliminar el dispositivo del grupo si ha estado inactivo por más de (días)**

     Si esta opción está habilitada, puede especificar el intervalo de tiempo que se deja pasar antes de que el dispositivo se elimine del grupo automáticamente. De forma predeterminada, esta opción se propaga a los grupos secundarios. El intervalo de tiempo por defecto es de 7 días.

     Esta opción está activada de forma predeterminada.
   - **Heredar del grupo primario**

     Si esta opción está habilitada, el período de retención de dispositivos en el grupo seleccionado se heredará del grupo primario y no se podrá modificar.

     Esta opción solo está disponible para grupos secundarios.

     Esta opción está activada de forma predeterminada.
   - **Forzar herencia en grupos secundarios**

     Los valores de configuración se propagarán a los grupos secundarios. Los ajustes correspondientes estarán bloqueados en las propiedades de esos grupos.

     Esta opción está deshabilitada de forma predeterminada.
4. Haga clic en el botón **Aceptar**.

Se guardarán y aplicarán los cambios.

## Inventario de equipos

La lista de hardware (**Operaciones** → **Repositorios** → **Hardware**) que usa para hacer un inventario del equipamiento se completa de dos formas: automática y manualmente. Después de cada sondeo de la red, todos los dispositivos que se detectan se agregan a la lista automáticamente; sin embargo, también puede agregar los dispositivos de forma manual si no desea sondear la red. Puede agregar otros dispositivos a la lista de forma manual, como routers, impresoras o hardware del dispositivo.

En las propiedades de un dispositivo puede ver y editar información detallada acerca de ese dispositivo.

La lista de hardware puede incluir los siguientes tipos de dispositivos:

- Equipos
- Dispositivos móviles
- Dispositivos de red
- Dispositivos virtuales
- Componentes OEM
- Periféricos de equipos
- Dispositivos conectados
- Teléfonos de VoIP
- Repositorios de red

El administrador puede asignar el atributo de *Equipo de empresa* a los dispositivos detectados. Este atributo puede asignarse manualmente en las propiedades de un dispositivo o el administrador puede especificar los criterios para que los atributos se asignen automáticamente. En este caso, el atributo de *Equipo de empresa* se asigna por tipo de dispositivo.

Kaspersky Security Center permite cancelar equipos. Para hacer esto, seleccione la opción **Cancelado** en las propiedades del dispositivo. Ese dispositivo no se muestra en la lista de equipos.

Un administrador puede administrar la lista de controladores lógicos programables (PLC) en la carpeta **Hardware**. Encontrará información detallada para administrar la lista de PLC en la *Guía para usuarios de Kaspersky Industrial Cyber Security for Nodes*.

## Agregar información sobre los dispositivos nuevos

*Para agregar información acerca de nuevos dispositivos en la red:*

1. En el menú principal, vaya a **Operaciones → Repositorios → Hardware**.
2. Haga clic en el botón **Agregar** para abrir la ventana **Nuevo dispositivo**.
3. En la ventana **Nuevo dispositivo**, en la lista desplegable **Tipo de dispositivo**, seleccione un tipo de dispositivo que desee agregar.
4. Haga clic en **Aceptar**.

   La ventana de Propiedades del dispositivo se abre en la sección **General**.

5. En la sección **General** complete los campos de entrada con datos del dispositivo. La sección **General** detalla la siguiente configuración:

   - **Dispositivo de la empresa**. Seleccione esta casilla si desea asignarle el atributo *Empresa* al dispositivo. Mediante este atributo, puede buscar dispositivos en la carpeta **Hardware**.
   - **Cancelado**. Seleccione esta casilla si no desea que el dispositivo figure en la lista de dispositivos de la carpeta **Hardware**.

6. Haga clic en **Aplicar**.

El nuevo dispositivo se mostrará en el espacio de trabajo de la página **Hardware**.

### Configurar criterios usados para los dispositivos de empresa

*Para configurar los criterios de detección para los dispositivos de empresa:*

1. En el menú principal, vaya a **Operaciones** → **Repositorios** → **Hardware**.
2. En la parte superior de la página **Hardware**, haga clic en el vínculo **Configurar regla para dispositivos de empresa**.

   Se invoca el panel **Configurar regla para dispositivos de empresa**.
3. En el panel **Configurar regla para dispositivos de empresa**, habilite la opción **Establecer el atributo del dispositivo de la empresa de forma automática**. Especifique los tipos de dispositivos a los que se les asigna automáticamente el atributo *Empresa*.

   Esta opción afecta solo a los dispositivos agregados a través del sondeo de red. Para los dispositivos agregados manualmente, configure el atributo *Empresa* manualmente.
4. Haga clic en **Aceptar**.

Se configuran los criterios de detección para dispositivos empresariales.

# Aplicaciones de Kaspersky: licencias y activación

Esta sección describe las funciones de Kaspersky Security Center relacionadas con el manejo de claves de licencia de las aplicaciones administradas de Kaspersky.

Kaspersky Security Center le permite realizar una distribución centralizada de las claves de licencia de las aplicaciones de Kaspersky en dispositivos cliente, supervisar su uso y renovar las licencias.

Al agregar una clave de licencia mediante Kaspersky Security Center, las propiedades de la clave de licencia se guardan en el Servidor de administración. Los parámetros definidos en las propiedades de las claves de licencia permiten que la aplicación genere un informe sobre el uso de las claves de licencia, mantenga al administrador al tanto de la caducidad de las licencias y le informe si se infringe una restricción dispuesta por una licencia. Puede configurar notificaciones sobre el uso de las claves de licencia en los ajustes del Servidor de administración.

# Licencias de aplicaciones administradas

Las aplicaciones de Kaspersky instaladas en los dispositivos administrados se deben licenciar aplicando un archivo de clave o código de activación a cada una de las aplicaciones. Los archivos de clave o códigos de activación se pueden desplegar de las siguientes formas:

- Despliegue automático
- Usar el paquete de instalación de la aplicación administrada
- La tarea *Agregar clave de licencia* para una aplicación administrada
- Activar la aplicación administrada manualmente

Puede agregar una nueva clave de licencia activa o de reserva mediante cualquiera de los métodos enumerados anteriormente. Una aplicación de Kaspersky utiliza una clave activa en el momento actual y almacena una clave de reserva para aplicar después de que caduque la clave activa. La aplicación para la que agrega una clave de licencia define si la clave está activa o si es de reserva. La definición de la clave no depende del método que utilice para agregar una nueva clave de licencia.

## Despliegue automático

Si usa diferentes aplicaciones administradas y tiene que desplegar un archivo de clave o un código de activación específicos en los dispositivos, opte por otras formas de desplegar ese código de activación o archivo de clave.

Kaspersky Security Center le permite desplegar las claves de licencia disponibles a los dispositivos automáticamente. Suponga, por ejemplo, que tiene tres claves de licencia en el repositorio del Servidor de administración. Ha seleccionado la casilla de verificación **Distribuir la clave de licencia automáticamente a los dispositivos administrados** para las tres claves de licencia. Los dispositivos de su organización tienen instalada una aplicación de seguridad de Kaspersky (por ejemplo, Kaspersky Endpoint Security para Windows). Se detecta un nuevo dispositivo al que se debe desplegar una clave de licencia. La aplicación determina, por ejemplo, que dos de las claves de licencia del repositorio se pueden desplegar en el dispositivo: una clave de licencia llamada *Clave_1* y una clave de licencia llamada *Clave_2*. Una de estas claves de licencia se despliega al dispositivo. En este caso, no se puede predecir cuál de las dos claves de licencia se desplegará en el dispositivo porque el despliegue automático de claves de licencia no proporciona ninguna actividad de administrador.

Cuando se despliega una clave de licencia, los dispositivos se vuelven a contar para esa clave de licencia. Debe asegurarse de que la cantidad de dispositivos a los que se desplegó la clave de licencia no exceda el límite de la licencia. Si la cantidad de dispositivos excede el límite de la licencia, a todos los dispositivos que no estaban cubiertos por la licencia se les asignará el estado *Crítico*.

Antes del despliegue, se deben agregar el archivo de clave o el código de activación al repositorio del Servidor de administración.

Instrucciones:

- Consola de administración:
  - Agregar una clave de licencia al repositorio del Servidor de administración
  - Distribución automática de una clave de licencia

  o
- Kaspersky Security Center Web Console:
  - Agregar una clave de licencia al repositorio del Servidor de administración
  - Distribución automática de una clave de licencia

Tenga en cuenta que una clave de licencia distribuida automáticamente podría no aparecer en el repositorio del Servidor de administración virtual en los siguientes casos:

- La clave de licencia no es válida para la aplicación.
- El Servidor de administración virtual no tiene ningún dispositivo administrado.
- La clave de licencia ya ha sido utilizada para dispositivos administrados asociados a otro Servidor de administración virtual y se ha alcanzado el límite a la cantidad de dispositivos.

## Adición de un archivo de clave o un código de activación al paquete de instalación de una aplicación administrada

Por motivos de seguridad, no se recomienda utilizar esta opción. El archivo de clave o el código de activación añadidos a un paquete de instalación pueden verse comprometidos.

Si instala una aplicación administrada con un paquete de instalación, puede especificar un código de activación o un archivo de clave en este paquete de instalación o en la directiva de la aplicación. En ese caso, la clave de licencia se desplegará a los dispositivos administrados cuando estos se sincronicen nuevamente con el Servidor de administración.

Instrucciones:

- Consola de administración:
  - Creación del paquete de instalación
  - Instalar aplicaciones en dispositivos cliente

  o
- Kaspersky Security Center Web Console: Adición de una clave de licencia a un paquete de instalación

### Despliegue con la tarea “Agregar clave de licencia” para una aplicación administrada

Si opta por usar la tarea *Agregar clave de licencia* para una aplicación administrada, puede seleccionar la clave que debe distribuirse a los dispositivos y seleccionar los dispositivos con comodidad, por ejemplo, seleccionando un grupo de administración o una selección de dispositivos.

Antes del despliegue, se deben agregar el archivo de clave o el código de activación al repositorio del Servidor de administración.

Instrucciones:

- Consola de administración:
  - Agregar una clave de licencia al repositorio del Servidor de administración
  - Distribución de claves de licencia a dispositivos cliente

  o
- Kaspersky Security Center Web Console:
  - Agregar una clave de licencia al repositorio del Servidor de administración
  - Distribución de claves de licencia a dispositivos cliente

### Agregar un código de activación o un archivo de clave en los dispositivos manualmente

Puede activar la aplicación de Kaspersky en forma local, usando las herramientas disponibles en la interfaz de la aplicación. Consulte la documentación de la aplicación instalada.

## Agregar una clave de licencia al repositorio del Servidor de administración

*Para agregar una clave de licencia al repositorio del Servidor de administración:*

1. Vaya a **Operaciones** → **Licencias** → **Licencias de Kaspersky**.
2. Haga clic en el botón **Agregar**.
3. Elija lo que quiera agregar:
   - **Agregar archivo de clave**

     Haga clic en el botón **Seleccionar archivo de clave** y vaya al archivo de clave que desea agregar.
   - **Escribir código de activación**

     Introduzca el código de activación en el campo de texto y haga clic en el botón **Enviar**.
4. Haga clic en el botón **Cerrar**.

Se agrega la clave de licencia (o las claves de licencia) al repositorio del Servidor de administración.

# Agregar una clave de licencia del Servidor de administración

*Para agregar una clave de licencia del Servidor de administración:*

1. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
2. En la ventana de propiedades del Servidor de administración que se abre, seleccione la sección **Claves de licencia**.
3. En la sección **Clave de licencia activa**, haga clic en el botón **Editar**.
4. En la ventana que se abre, haga clic en el botón **Agregar** para agregar una clave de licencia.

   Se inicia el asistente Agregar clave de licencia.

Una vez finalizado el asistente, puede verificar si las funciones se muestran en la Consola de administración de acuerdo con la licencia correspondiente.

# Distribución de claves de licencia a dispositivos cliente

Kaspersky Security Center Web Console permite distribuir una clave de licencia a los dispositivos cliente automáticamente o mediante la tarea de **Activación de la aplicación**. Con la tarea, puede distribuir claves a un grupo de dispositivos específico. Durante la distribución de una clave de licencia mediante una tarea, no se tiene en cuenta el límite de obtención de licencias en el número de dispositivos. Use la distribución automática de claves para detener la distribución de una clave de licencia automáticamente cuando se alcance el límite de obtención de licencias.

Si habilita la opción Distribución automática de una clave de licencia, no cree una tarea de **Activación de la aplicación** para distribuir la clave a los dispositivos cliente. De lo contrario, la carga en el Servidor de administración aumentará debido a la frecuencia de la sincronización.

Antes de realizar la distribución, agregue la clave de licencia al repositorio del Servidor de administración.

*Para distribuir una clave de licencia a los dispositivos cliente con la tarea de **Activación de la aplicación**:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el **Asistente para crear nueva tarea**. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
3. En la lista desplegable **Aplicación**, seleccione la aplicación para la que desee agregar una clave de licencia.
4. En la lista **Tipo de tarea**, seleccione la tarea de **Activación de la aplicación**.
5. En el campo **Nombre de la tarea**, ingrese el nombre de la tarea nueva.
6. Seleccione los dispositivos a los que se asignará la tarea.

7. En el paso **Seleccionar una clave de licencia** del asistente, haga clic en el vínculo **Agregar clave** para agregar la clave de licencia.

8. En el panel para agregar claves, agregue la clave de licencia mediante una de las siguientes opciones:

   Debe agregar la clave de licencia solo si no la agregó al repositorio del Servidor de administración antes de crear la tarea de **Activación de la aplicación**.

   - Seleccione la opción **Escribir código de activación** para ingresar un código de activación y luego haga lo siguiente:

     a. Especifique el código de activación y haga clic en el botón **Enviar**.

     La información sobre la clave de licencia aparece en el panel para agregar claves.

     b. Haga clic en el botón **Guardar**.

     Si desea distribuir la clave de licencia a los dispositivos administrados de forma automática, habilite la opción **Distribuir la clave de licencia automáticamente a los dispositivos administrados**.

     Se cerrará el panel para agregar claves.

   - Seleccione la opción **Agregar archivo de clave** para agregar un archivo de clave y luego haga lo siguiente:

     a. Haga clic en el botón **Seleccionar archivo de clave**.

     b. En la ventana que se abre, seleccione un archivo de clave y haga clic en el botón **Abrir**.

     La información sobre la clave de licencia aparecerá en el panel para agregar claves de licencia.

     c. Haga clic en el botón **Guardar**.

     Si desea distribuir la clave de licencia a los dispositivos administrados de forma automática, habilite la opción **Distribuir la clave de licencia automáticamente a los dispositivos administrados**.

     Se cerrará el panel para agregar claves.

9. Seleccione la clave de licencia desde la tabla de claves.

10. En el paso **Información de licencia** del asistente, desmarque la casilla **Usar como clave de reserva** predeterminada si desea reemplazar la clave de licencia activa.

    Por ejemplo, puede ser necesario cuando la organización cambia y se necesita la clave de otra organización en el dispositivo o si la clave se volvió a emitir y la nueva licencia caduca antes que la licencia actual. Para evitar errores, debe desmarcar la casilla **Usar como clave de reserva**.

    Si desea obtener más información sobre las cuestiones que pueden surgir al agregar una clave de licencia a Kaspersky Security Center y cómo resolverlas, consulte la Base de conocimientos de Kaspersky Security Center.

11. En el paso **Finalizar la creación de la tarea** del asistente, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** para modificar la configuración predeterminada de la tarea.

    Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificarla más adelante.

12. Haga clic en el botón **Finalizar**.

    El asistente creará la tarea. Si habilitó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abrirá automáticamente la ventana de propiedades de la tarea. En esta ventana, puede definir la configuración general de la tarea y, si es necesario, cambiar los ajustes establecidos durante la creación de la tarea.

    > También puede abrir la ventana de propiedades de la tarea haciendo clic en el nombre de la tarea creada en la lista de tareas.

    La tarea se creará, configurará y se mostrará en la lista de tareas.

13. Para ejecutar la tarea, selecciónela en la lista de tareas y haga clic en el botón **Iniciar**.

    También puede programar el inicio de la tarea en la pestaña **Programación**, en la ventana de propiedades de la tarea.

    Para obtener una descripción detallada de la configuración de inicio programado, consulte la configuración general de la tarea.

Cuando se complete la tarea, la clave de licencia se desplegará a los dispositivos seleccionados.

# Distribución automática de una clave de licencia

Kaspersky Security Center permite la distribución automática de claves de licencia a dispositivos administrados si están ubicadas en el repositorio de claves de licencia del Servidor de administración.

*Para distribuir una clave de licencia en forma automática a los dispositivos administrados:*

1. Vaya a **Operaciones** → **Licencias** → **Licencias de Kaspersky**.
2. Haga clic en el nombre de la clave de licencia que quiera que se distribuya a los dispositivos automáticamente.
3. En la ventana de propiedades de la clave de licencia que se abre, active la casilla de verificación **Distribuir la clave de licencia automáticamente a los dispositivos administrados**.
4. Haga clic en el botón **Guardar**.

La clave de licencia se distribuye automáticamente a todos los dispositivos compatibles.

La distribución de claves de licencia se realiza a través del Agente de red. No se crean tareas de distribución de clave de licencia para la aplicación.

Durante la distribución automática de una clave de licencia se tiene en cuenta el límite de obtención de licencias en el número de dispositivos. Este límite está definido en las propiedades de la clave de licencia. Cuando se llega al límite de dispositivos, el proceso de distribución se detiene automáticamente y la clave de licencia no se transfiere a más dispositivos.

Tenga en cuenta que una clave de licencia distribuida automáticamente podría no aparecer en el repositorio del Servidor de administración virtual en los siguientes casos:

- La clave de licencia no es válida para la aplicación.
- El Servidor de administración virtual no tiene ningún dispositivo administrado.
- La clave de licencia ya ha sido utilizada para dispositivos administrados asociados a otro Servidor de administración virtual y se ha alcanzado el límite a la cantidad de dispositivos.

El Servidor de administración virtual distribuye automáticamente las claves de licencia desde su repositorio y desde el repositorio del Servidor de administración. Le sugerimos que atienda a las siguientes recomendaciones:

- Use la tarea *Agregar clave de licencia* para seleccionar la clave de licencia que se debe distribuir a los dispositivos.
- Evite deshabilitar la opción **Permitir el despliegue automático de claves de licencia de este Servidor de administración virtual a sus dispositivos** en la configuración del Servidor de administración virtual. De lo contrario, el Servidor de administración virtual no distribuirá claves de licencia a los dispositivos, incluidas las claves de licencia del repositorio del Servidor de administración.

Si selecciona la casilla de verificación **Distribuir la clave de licencia automáticamente a los dispositivos administrados** en la ventana de propiedades de la clave de licencia, se distribuye una clave de licencia en su red inmediatamente. Si no selecciona esta opción, puede distribuir una clave de licencia manualmente más adelante con una tarea.

La distribución automática de las claves de licencia configuradas en el Servidor de administración principal no se extiende a los dispositivos administrados por Servidores de administración secundarios no virtuales.

# Visualización de información sobre las claves de licencia en uso

*Para ver la lista de las claves de licencia agregadas al repositorio del Servidor de administración:*

Vaya a **Operaciones** → **Licencias** → **Licencias de Kaspersky**.

Se mostrará una lista con los archivos de clave y los códigos de activación que se hayan agregado al repositorio del Servidor de administración.

*Para ver información detallada sobre una clave de licencia:*

1. Vaya a **Operaciones** → **Licencias** → **Licencias de Kaspersky**.
2. Haga clic en el nombre de la clave de licencia de su interés.

Se abre una ventana con las propiedades de la clave de licencia. En la ventana, puede ver lo siguiente:

- En la pestaña **General**, los datos generales de la clave de licencia.
- en la pestaña **Dispositivos**, la lista de dispositivos cliente en los que la clave de licencia se utilizó para activar la aplicación de Kaspersky instalada.

*Para ver qué claves de licencia se despliegan en un dispositivo cliente específico:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.
2. Haga clic en el nombre del dispositivo pertinente.
3. En la ventana que se abre, que contendrá las propiedades del dispositivo, elija la pestaña **Aplicaciones**.
4. Haga clic en el nombre de la aplicación para la que desea ver la información sobre la clave de licencia.
5. En la ventana de propiedades de la aplicación que se abre, seleccione la pestaña **General** y, luego, abra la sección **Licencia**.

Se muestra la información principal sobre las claves de licencia de reserva y activas.

Para definir la configuración actualizada de las claves de licencia del Servidor de administración virtual, este envía una solicitud a los servidores de activación de Kaspersky como mínimo una vez al día. Si los servidores DNS configurados en el sistema no permiten acceder a los servidores de Kaspersky, la aplicación utiliza servidores DNS públicos.

# Eliminar una clave de licencia del repositorio

Cuando elimina la clave de licencia activa para una función adicional del Servidor de administración, por ejemplo Administración de vulnerabilidades y parches o Administración de dispositivos móviles, la función correspondiente deja de estar disponible. Si agregó una clave de licencia de reserva, al eliminar la clave de licencia activa, la clave de reserva se convertirá automáticamente en la clave de licencia activa.

Cuando elimina la clave de licencia activa desplegada en un dispositivo administrado, la aplicación continúa trabajando en el dispositivo administrado.

*Para eliminar un archivo de clave o un código de activación del repositorio del Servidor de administración:*

1. Verifique que el Servidor de administración no esté utilizando el archivo de clave o el código de activación que desee eliminar. Si el Servidor de administración está utilizando ese archivo o código, no lo podrá eliminar. Para realizar la verificación, haga lo siguiente:
   a. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

      Se abre la ventana Propiedades del Servidor de administración.

   b. En la pestaña **General**, vaya a la sección **Claves de licencia**.
   c. Si ve el archivo de clave o el código de activación que desea eliminar en esta sección, haga clic en el botón **Eliminar clave de licencia activa** y confirme la operación. El Servidor de administración dejará de utilizar la clave de licencia eliminada, pero no se la borrará del repositorio del Servidor de administración. Si el archivo de clave o el código de activación que desea eliminar no aparecen en esta sección, sabrá que no son el archivo o código utilizados por el Servidor de administración.
2. En el menú principal, vaya a **Operaciones** → **Licencias** → **Licencias de Kaspersky**.
3. Seleccione el archivo de clave o el código de activación pertinentes y haga clic en el botón **Eliminar**.

El archivo de clave o el código de activación que haya seleccionado se eliminará del repositorio.

Puede volver a agregar una clave de licencia eliminada o agregar una clave de licencia nueva.

# Revocar la aceptación de un Contrato de licencia de usuario final

Si ya no necesita proteger un dispositivo cliente, puede revocar el Contrato de licencia de usuario final (EULA) vinculado a la aplicación de Kaspersky administrada que ese dispositivo tenga instalada. Antes de revocar un EULA, deberá desinstalar la aplicación a la que el contrato esté asociado.

Los EULA aceptados en un Servidor de administración virtual pueden revocarse en dicho servidor o en el Servidor de administración principal. Los EULA aceptados en un Servidor de administración principal únicamente se pueden revocar en ese mismo Servidor de administración principal.

*Para revocar un EULA vinculado a una aplicación de Kaspersky administrada:*

1. Abra la ventana de propiedades del Servidor de administración y, en la pestaña **General**, elija la sección **Contratos de licencia de usuario final**.

   Se muestra una lista con los EULA aceptados tras la creación de paquetes de instalación, la instalación sin problemas de actualizaciones o el despliegue de Kaspersky Security para dispositivos móviles.

2. En la lista, seleccione el EULA que desee revocar.

   Puede ver las siguientes propiedades del EULA:

   - La fecha en la que se aceptó el EULA.
   - El nombre del usuario que aceptó el EULA.

3. Haga clic en la fecha de aceptación de un EULA para abrir una ventana de propiedades con la siguiente información:

   - El nombre del usuario que aceptó el EULA.
   - La fecha en la que se aceptó el EULA.
   - El identificador único (UID) del EULA.
   - El texto completo del EULA.
   - La lista de objetos vinculados al EULA (paquetes de instalación, actualizaciones transparentes, apps móviles). Junto al nombre de cada objeto, verá de qué tipo de objeto se trata.

4. En la parte izquierda de la ventana de propiedades del EULA, haga clic en el botón **Revocar el Contrato de licencia**.

   > De existir algún objeto que impida revocar el EULA (algún paquete de instalación con su respectiva tarea), verá una notificación. No podrá revocar el contrato hasta que haya eliminado el objeto problemático.

   En la ventana que se abre, se le informa que primero debe desinstalar la aplicación de Kaspersky correspondiente al EULA.

5. Haga clic en el botón para confirmar la revocación.

Se revoca el EULA. En la lista de la sección **Contratos de licencia de usuario final**, desaparece la entrada correspondiente al contrato. La ventana de propiedades del EULA se cierra; la aplicación ya no está instalada.

# Renovación de licencias para aplicaciones de Kaspersky

Puede renovar la licencia de una aplicación de Kaspersky que ya haya caducado o que esté próxima a caducar (que caduque en menos de treinta días).

*Para renovar una licencia caducada o una licencia que está a punto de caducar:*

1. Realice alguna de las siguientes acciones:

   - En el menú principal, vaya a **Operaciones → Licencias → Licencias de Kaspersky**.
   - En el menú principal, vaya a **Supervisión e informes → Panel** y, luego, haga clic en el vínculo **Ver licencias por caducar** junto a una notificación.

   Se abre la ventana **Licencias de Kaspersky**, donde puede ver y renovar las licencias.

2. Haga clic en el enlace **Renovar licencia** ubicado junto a la licencia pertinente.

   Al hacer clic en un enlace de renovación de licencia, acepta transferir a Kaspersky la siguiente información sobre Kaspersky Security Center: la versión, la ubicación utilizada, el ID de la licencia del software (es decir, el ID de la licencia que está renovando) y si compró la licencia a través de una empresa asociada o no.

3. Se abrirá una ventana del servicio de renovación de licencias. Siga las instrucciones para renovar la licencia.

   Se renueva la licencia.

Cuando una licencia esté próxima a caducar, Kaspersky Security Center Web Console mostrará una notificación siguiendo este esquema:

- 30 días antes de la caducidad
- 7 días antes de la caducidad
- 3 días antes de la caducidad
- 24 horas antes de la caducidad
- Cuando la licencia haya caducado

# Utilizar Kaspersky Marketplace para elegir soluciones empresariales de Kaspersky

**Marketplace** es una sección del menú principal en la que puede ver el catálogo completo de soluciones empresariales de Kaspersky, seleccionar las soluciones que necesita y adquirir esos productos en el sitio web de Kaspersky. Puede utilizar filtros para ver solo las soluciones que resulten adecuadas para su organización y para los requisitos de su sistema de seguridad de la información. Cuando selecciona una solución, Kaspersky Security Center lo redirige a la página web relacionada en el sitio web de Kaspersky para obtener más información sobre esa solución. Allí podrá proceder con la compra o ver instrucciones sobre el proceso de compra.

Puede usar los siguientes criterios para filtrar las soluciones de Kaspersky que se muestran en la sección **Marketplace**:

- Número de dispositivos (endpoints, servidores y otros tipos de activos) que desea proteger:
  - 50–250
  - 250-1000
  - Más de 1000
- Nivel de madurez del equipo de seguridad de la información de su organización:
  - **Foundations**

    Este es el nivel típico de las empresas que solo tienen un equipo de TI. Se bloqueará la mayor cantidad de amenazas posible en forma automática.
  - **Optimum**

    Este es el nivel típico de las empresas que, dentro de su equipo de TI, tienen personal específicamente a cargo de la seguridad informática. En este nivel, las empresas necesitan soluciones que les permitan contrarrestar tanto amenazas básicas como amenazas que puedan eludir sus mecanismos de prevención existentes.
  - **Expert**

    Este es el nivel típico de las empresas que tienen entornos de TI complejos y distribuidos. Estas empresas tienen un equipo de seguridad informática experimentado o un centro de operaciones de seguridad (SOC). En este nivel, las empresas necesitan soluciones que les permitan contrarrestar amenazas complejas y ataques dirigidos.
- Tipos de activos que desea proteger:
  - **Endpoints**: estaciones de trabajo utilizadas por los empleados, máquinas físicas y virtuales, sistemas integrados
  - **Servidores**: servidores físicos y virtuales
  - **Nube**: entornos de nube pública, privada o híbrida; servicios en la nube
  - **Red**: red de área local, infraestructura de TI
  - **Servicios**: servicios relacionados con la seguridad proporcionados por Kaspersky

*Para buscar y comprar una solución empresarial de Kaspersky:*

1. En el menú principal, vaya a **Marketplace**.

   De forma predeterminada, la sección muestra todas las soluciones empresariales de Kaspersky disponibles.

2. Para ver solo aquellas soluciones que sean adecuadas para su organización, seleccione los valores pertinentes en los filtros.

3. Haga clic en la solución que desee comprar o investigar en más detalle.

   Será redirigido a la página web de la solución. Puede seguir las instrucciones en pantalla para proceder con la compra.

# Configurar la protección de la red

En esta sección, encontrará información sobre la configuración manual de tareas y directivas, sobre los roles de usuario y sobre la creación de una jerarquía de tareas y una estructura de grupos de administración.

# Procedimiento: Configurar la protección de la red

El asistente de inicio rápido crea directivas y tareas con la configuración predeterminada. Esta configuración podría ser subóptima (o incluso inadmisible) para su organización. Por este motivo, recomendamos que modifique estas directivas y tareas predeterminadas y que, de ser necesario, cree otras directivas y tareas adicionales para su red.

## Requisitos previos

Antes de comenzar, compruebe que hizo lo siguiente:

- Instaló el Servidor de administración de Kaspersky Security Center
- Kaspersky Security Center Web Console instalada (opcional)
- Completado el escenario de instalación principal de Kaspersky Security Center
- Completó todos los pasos del asistente de inicio rápido o creó manualmente las siguientes directivas y tareas en el grupo de administración **Dispositivos administrados**:
  - Directiva de Kaspersky Endpoint Security
  - Tarea de grupo para actualizar Kaspersky Endpoint Security
  - Directiva del Agente de red
  - Tarea *Buscar vulnerabilidades y actualizaciones requeridas*

El proceso para configurar la protección de la red se divide en etapas:

1. **Configurar y propagar directivas y perfiles de directivas para las aplicaciones de Kaspersky**

Para configurar y propagar la configuración de las aplicaciones Kaspersky instaladas en los dispositivos administrados, puede utilizar dos enfoques de la gestión de la seguridad diferentes: centrada en el dispositivo o centrada en el usuario. Estos dos enfoques también se pueden combinar. Para implementar la administración de seguridad centrada en el dispositivo, puede usar las herramientas proporcionadas en la Consola de administración basada en Microsoft Management Console o en Kaspersky Security Center Web Console. La administración de la seguridad centrada en el usuario solamente se puede implementar a través de Kaspersky Security Center Web Console.

2. **Configurar tareas para administrar las aplicaciones de Kaspersky en forma remota**

   Revise las tareas creadas con el asistente de inicio rápido y modifique sus ajustes según corresponda.

   Instrucciones:

   - Consola de administración:
     - Configuración de la tarea de grupo para actualizar Kaspersky Endpoint Security
     - Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas
   - Kaspersky Security Center Web Console:
     - Configuración de la tarea de grupo para actualizar Kaspersky Endpoint Security
     - Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

   Si es necesario, cree tareas adicionales para administrar las aplicaciones Kaspersky instaladas en los dispositivos cliente.

3. **Evaluar y limitar el impacto de los eventos en la base de datos**

   Se transfiere la información sobre eventos que ocurren durante el funcionamiento de aplicaciones administradas de un dispositivo cliente y se la registra en la base de datos del Servidor de administración. Para reducir la carga en el Servidor de administración, evalúe y limite el número máximo de eventos que se pueden almacenar en la base de datos.

   Instrucciones:

   - Consola de administración: Establecer el número máximo de eventos
   - Kaspersky Security Center Web Console: Configuración del número máximo de eventos

## Resultados

Al concluir este escenario, su red estará protegida a través de la configuración de las aplicaciones de Kaspersky, de las distintas tareas y de los eventos recibidos por el Servidor de administración:

- Las aplicaciones de Kaspersky tendrán la configuración definida en las directivas y en los perfiles de directivas.
- Las aplicaciones se administrarán a través de un grupo de tareas.
- Habrá un límite a la cantidad de eventos almacenados en la base de datos.

Una vez que termine de configurar la protección para su red, asegúrese de que las bases de datos y las aplicaciones de Kaspersky se actualicen en forma periódica.

Para obtener detalles sobre cómo configurar las respuestas automáticas a las amenazas detectadas por Kaspersky Sandbox, consulte la Ayuda en línea de Kaspersky Sandbox 2.0.

# Acerca de la administración de la seguridad centrada en el dispositivo y centrada en el usuario

Puede administrar los ajustes de seguridad utilizando dos enfoques o perspectivas diferentes. Uno de estos enfoques pone el eje en las características de los dispositivos; el otro, en los roles de los usuarios. El primer enfoque se denomina *administración de la seguridad centrada en el dispositivo*, mientras que el segundo recibe el nombre de *administración de la seguridad centrada en el usuario*. Puede usar cualquiera de estos métodos (o ambos en conjunto) para configurar sus aplicaciones de maneras diferentes en dispositivos diferentes. Para implementar la administración de seguridad centrada en el dispositivo, puede usar las herramientas proporcionadas en la Consola de administración basada en Microsoft Management Console o en Kaspersky Security Center Web Console. La administración de la seguridad centrada en el usuario solamente se puede implementar a través de Kaspersky Security Center Web Console.

El enfoque centrado en el dispositivo permite que la configuración de una aplicación de seguridad varíe según las características del dispositivo administrado en el que se encuentra instalada. Es posible, por ejemplo, definir ajustes de configuración diferentes para dispositivos asignados a grupos de administración diferentes. Los dispositivos también pueden diferenciarse sobre la base de sus especificaciones de hardware o de su uso en Active Directory.

El enfoque centrado en el usuario permite configurar las aplicaciones de seguridad de maneras diferentes para roles de usuario diferentes. Puede crear una serie de roles de usuario, asignarlos a sus usuarios según las funciones que desempeñen en la empresa y luego crear configuraciones diferentes, que se apliquen a uno u otro dispositivo según el rol asignado al propietario del dispositivo. Imagine, por ejemplo, que una aplicación de Kaspersky debe estar configurada de un modo diferente si se encuentra instalada en el dispositivo de un contador o en el dispositivo de un especialista en RR. HH. Al implementar la administración de la seguridad centrada en el usuario, puede hacer que cada departamento (el de Contabilidad y el de Recursos Humanos) tenga su propio "juego de ajustes" para esa aplicación. El juego de ajustes determina qué valores de configuración pueden ser modificados por los usuarios y cuáles se imponen por la fuerza y solamente pueden ser modificados por el administrador.

El enfoque centrado en el usuario también permite configurar una aplicación de un modo específico para un usuario específico. Esto puede ser útil si hay un empleado con un rol único en la empresa o si se quieren supervisar los problemas de seguridad asociados a los dispositivos de una persona en particular. El rol de este empleado en particular podría determinar si la persona tendrá más o menos derechos para modificar los ajustes de la aplicación. Un administrador de sistemas que tenga a su cargo los dispositivos cliente de una oficina local podría necesitar más derechos que otros usuarios.

El enfoque centrado en el dispositivo y el enfoque centrado en el usuario pueden combinarse. Podría, por ejemplo, configurar una directiva de aplicación específica para cada uno de sus grupos de administración y, luego, podría crear perfiles de directivas que se apliquen a uno o más de los roles de usuario definidos en su empresa. Si hace esto, las directivas y los perfiles se aplicarán en el siguiente orden:

1. Se aplicarán las directivas creadas en el marco del enfoque centrado en el dispositivo.
2. Los perfiles modificarán las directivas siguiendo el orden de prioridad definido para los perfiles de directivas.
3. Los perfiles de directivas vinculados a los roles de usuario modificarán las directivas.

# Configuración y propagación de directivas: enfoque centrado en el dispositivo

Cuando complete este proceso, las aplicaciones de sus dispositivos administrados estarán configuradas a través de las directivas y los perfiles de directiva que usted defina.

## Requisitos previos

Antes de comenzar, asegúrese de haber instalado correctamente el Servidor de administración de Kaspersky Security Center y Kaspersky Security Center Web Console (opcional). Si instaló Kaspersky Security Center Web Console, es posible que también desee considerar la administración de seguridad centrada en el usuario como una opción alternativa o adicional al enfoque centrado en el dispositivo.

## Etapas

El proceso para administrar las aplicaciones de Kaspersky utilizando un enfoque centrado en el dispositivo se divide en los siguientes pasos:

1. **Configurar directivas para las aplicaciones**

   Cree y configure una directiva para cada aplicación de Kaspersky que se encuentre instalada en los dispositivos administrados. Estas directivas se propagarán a los dispositivos cliente.

   Cuando se utiliza el asistente de inicio rápido para configurar la protección de la red, Kaspersky Security Center crea una directiva predeterminada para las siguientes aplicaciones:

   - Kaspersky Endpoint Security para Windows (para dispositivos cliente con Windows)
   - Kaspersky Endpoint Security for Linux (para dispositivos cliente con Linux)

   Si completó el proceso de configuración utilizando este asistente, no es necesario que cree una nueva directiva para esta aplicación. Lleve a cabo la configuración manual de la directiva de Kaspersky Endpoint Security.

   Si tiene una estructura jerárquica de varios Servidores de administración o grupos de administración, los Servidores de administración secundarios y los grupos de administración secundarios heredan las directivas del Servidor de administración principal de forma predeterminada. Puede forzar la herencia de los grupos secundarios y los Servidores de administración secundarios para prohibir cualquier modificación de los ajustes configurados en la directiva ascendente. Si desea que solo algunos de los ajustes se hereden por la fuerza, bloquee esos ajustes en la directiva de nivel superior. El resto de configuraciones desbloqueadas estarán disponibles para modificación en las directivas posteriores. La jerarquía de directivas resultante le será de gran utilidad para gestionar los dispositivos de los grupos de administración.

   Instrucciones:

   - Consola de administración: Creación de una directiva
   - Kaspersky Security Center Web Console: Crear una directiva

2. **Crear perfiles de directivas (opcional)**

Si desea que los dispositivos de un mismo grupo de administración estén sujetos a distintos ajustes de directivas, puede crear perfiles de directivas para esos dispositivos. Un perfil de directiva es un subconjunto nominado de los valores de configuración definidos en una directiva. Este subconjunto de valores, que se distribuye a los dispositivos de destino junto con la propia directiva, entra en vigor cuando se presenta una condición específica, llamada *condición de activación del perfil*. Un perfil contiene solamente los valores de configuración que difieren de los de la directiva "básica" que se encuentra activa en el dispositivo administrado.

A través de las condiciones de activación, podrá aplicar perfiles de directivas diferentes a, por ejemplo, los dispositivos que pertenezcan a ciertas unidades o a ciertos grupos de seguridad de Active Directory, a los que tengan configuraciones de hardware específicas o a los que estén marcados con etiquetas específicas. Puede usar las etiquetas para filtrar dispositivos que reúnen criterios específicos. Podría, por ejemplo, crear una etiqueta llamada *Windows*, marcar con ella los dispositivos que utilicen el sistema operativo Windows y especificarla como condición de activación para un perfil de directiva. Ello hará que las aplicaciones de Kaspersky instaladas en dispositivos con Windows queden sujetas a un perfil de directiva específico.

Instrucciones:

- Consola de administración:
  - Crear un perfil de directiva
  - Crear una regla de activación para un perfil de directiva
- Kaspersky Security Center Web Console:
  - Crear un perfil de directiva
  - Crear una regla de activación para un perfil de directiva

3. **Propagar las directivas y los perfiles de directivas a los dispositivos administrados**

   De forma predeterminada, el Servidor de administración se sincroniza automáticamente con los dispositivos administrados cada 15 minutos. Puede evitar la sincronización automática y ejecutar la sincronización manualmente utilizando el comando Forzar sincronización. También se realiza una sincronización forzada cada vez que se crea o modifica una directiva o perfil de directiva. Las directivas nuevas o con cambios y los perfiles de directivas se propagan a los dispositivos administrados durante la sincronización.

   Si usa Kaspersky Security Center Web Console, puede verificar si las directivas y los perfiles de directivas se entregaron a un dispositivo. Kaspersky Security Center especifica la fecha y la hora de entrega en las propiedades del dispositivo.

   Instrucciones:

   - Consola de administración: sincronización forzada
   - Kaspersky Security Center Web Console: Sincronización forzada

## Resultados

Al concluir este proceso, las aplicaciones de Kaspersky tendrán la configuración especificada y propagada a través de la jerarquía de directivas.

Las directivas y los perfiles de directivas configurados para las aplicaciones se aplicarán automáticamente a los nuevos dispositivos que se agreguen a los grupos de administración.

# Configuración y propagación de directivas: enfoque centrado en el usuario

En esta sección se describe un proceso para configurar, de manera centralizada y tomando como eje a los usuarios, los ajustes de las aplicaciones de Kaspersky instaladas en los dispositivos administrados. Cuando complete este proceso, las aplicaciones de sus dispositivos administrados estarán configuradas a través de las directivas y los perfiles de directiva que usted defina.

Este escenario se puede implementar a través de Kaspersky Security Center Web Console versión 13 o posterior.

## Requisitos previos

Antes de comenzar, asegúrese de haber instalado correctamente el Servidor de administración de Kaspersky Security Center y Kaspersky Security Center Web Console y de haber completado el escenario de instalación principal. Para administrar la seguridad, considere también utilizar un enfoque centrado en el dispositivo, ya sea en reemplazo o como complemento de este enfoque centrado en el usuario. Más información sobre dos enfoques de administración.

## Proceso

El proceso para administrar las aplicaciones de Kaspersky utilizando un enfoque centrado en el usuario se divide en los siguientes pasos:

1. **Configurar directivas para las aplicaciones**

   Cree y configure una directiva para cada aplicación de Kaspersky que se encuentre instalada en los dispositivos administrados. Estas directivas se propagarán a los dispositivos cliente.

   Cuando configura la protección de su red en el Asistente de inicio rápido, Kaspersky Security Center crea la directiva predeterminada para Kaspersky Endpoint Security. Si completó el proceso de configuración utilizando este asistente, no es necesario que cree una nueva directiva para esta aplicación. En cambio, puede sencillamente configurar la directiva de Kaspersky Endpoint Security en forma manual.

   Si tiene una estructura jerárquica de varios Servidores de administración o grupos de administración, los Servidores de administración secundarios y los grupos de administración secundarios heredan las directivas del Servidor de administración principal de forma predeterminada. Puede forzar la herencia de los grupos secundarios y los Servidores de administración secundarios para prohibir cualquier modificación de los ajustes configurados en la directiva ascendente. Si desea que solo algunos de los ajustes se hereden por la fuerza, bloquee esos ajustes en la directiva de nivel superior. El resto de configuraciones desbloqueadas estarán disponibles para modificación en las directivas posteriores. La jerarquía de directivas resultante le será de gran utilidad para gestionar los dispositivos de los grupos de administración.

   Instrucciones: Crear una directiva

2. **Designar los propietarios de los dispositivos**

   Asigne los dispositivos administrados a los usuarios correspondientes.

   Instrucciones: Designación de un usuario como propietario de un dispositivo

3. **Definir los roles de usuario más usuales en la empresa**

Piense en las clases de labores que suele realizar el personal de su empresa. Debe dividir a los empleados basándose en las funciones o roles que cumplen. Puede hacer la división por departamento, profesión o cargo, por ejemplo. Tras hacer esta división, deberá crear un rol de usuario para cada grupo. Tenga en cuenta que cada rol de usuario tendrá su propio perfil de directiva, con ajustes de software que serán específicos para ese rol.

4. **Crear roles de usuario**

   Cree y configure una función de usuario para cada grupo de empleados que definió en el paso anterior o use las funciones de usuario predefinidos. Los roles de usuario contienen un conjunto de derechos que regulan el acceso a las funciones de las aplicaciones.

   Instrucciones: Creación de roles de usuario

5. **Definir el alcance de cada rol de usuario**

   Defina los usuarios, grupos de seguridad o grupos de administración de cada uno de los roles de usuario que haya creado. Los ajustes asociados a un rol de usuario se aplican únicamente a los dispositivos que pertenecen a los usuarios que tienen ese rol, y solo cuando esos dispositivos pertenecen a grupos y subgrupos asociados al rol en cuestión.

   Instrucciones: Editar el alcance de un rol de usuario

6. **Crear perfiles de directiva**

   Cree un perfil de directiva para cada rol de usuario que exista en su empresa. Los perfiles de directivas determinan qué ajustes de configuración corresponde utilizar en las aplicaciones instaladas en los dispositivos de los usuarios, tomando como parámetro el rol de cada usuario.

   Instrucciones: Crear un perfil de directiva

7. **Asociar los perfiles de directivas con los roles de usuario**

   Asocie los perfiles de directivas que haya creado con los distintos roles de usuario. De este modo, logrará que cada perfil de directiva se activará para los usuarios que tengan el rol especificado. Los ajustes configurados en cada perfil de directiva se implementarán en las aplicaciones de Kaspersky instaladas en los dispositivos de cada usuario.

   Instrucciones: Asociación de perfiles de directivas con roles

8. **Propagar las directivas y los perfiles de directivas a los dispositivos administrados**

   De forma predeterminada, el Servidor de administración se sincroniza automáticamente con los dispositivos administrados cada 15 minutos. Las directivas nuevas o con cambios y los perfiles de directivas se propagan a los dispositivos administrados durante la sincronización. Puede saltear la sincronización automática y realizar una sincronización manual a través del comando "Forzar sincronización". Una vez que se completa la sincronización, las directivas y los perfiles de directivas se entregan y aplican a las aplicaciones de Kaspersky instaladas.

   Puede verificar si las directivas y los perfiles de directivas se entregaron a un dispositivo. Kaspersky Security Center especifica la fecha y la hora de entrega en las propiedades del dispositivo.

   Instrucciones: Sincronización forzada

## Resultados

Al concluir este proceso, las aplicaciones de Kaspersky tendrán la configuración especificada y propagada a través de la jerarquía de directivas y perfiles de directivas.

Cuando necesite sumar un nuevo usuario, cree una cuenta nueva para esa persona y asígnele los dispositivos que usará y uno de los roles de usuario que haya creado. Las directivas y los perfiles de directivas que haya configurado para las aplicaciones se aplicarán automáticamente a los dispositivos del nuevo usuario.

# Ajustes de la directiva del Agente de red

*Para configurar la directiva del Agente de red:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva del Agente de red.

   Se abre la ventana de propiedades de la directiva del Agente de red.

Consulte la tabla comparativa que detalla cómo se aplican las configuraciones a continuación, según el tipo de sistema operativo utilizado.

## General

En la pestaña, puede modificar el estado de la directiva y especificar la herencia de la configuración de la directiva:

- En **Estado de la directiva**, puede seleccionar uno de los modos de la directiva:
  - **Activa**

    Si se selecciona esta opción, se activa la directiva.

    Esta opción está seleccionada de forma predeterminada.

  - **Inactiva**

    Si selecciona esta opción, la directiva estará inactiva, pero quedará guardada en la carpeta **Directivas**. Podrá activarla cuando resulte necesario.

- En el grupo de ajustes **Herencia de configuración**, puede configurar las opciones de directiva:
  - **Heredar configuración de la directiva primaria**

    Si habilita esta opción, la directiva heredará los valores de configuración definidos en la directiva del grupo de nivel superior. Estos valores, en consecuencia, estarán bloqueados.

    Esta opción está activada de forma predeterminada.

  - **Forzar la herencia de configuración en las directivas secundarias**

    Si habilita esta opción, cuando modifique la directiva y se apliquen los cambios, ocurrirá lo siguiente:
    - Los valores de configuración de la directiva se propagarán a las directivas de los subgrupos de administración (es decir, a las directivas secundarias).
    - En la ventana de propiedades de cada directiva secundaria, dentro del bloque **Herencia de configuración** de la sección **General**, se habilitará automáticamente la opción **Heredar configuración de la directiva primaria**.

    Habilitar esta opción hace que los ajustes de las directivas secundarias se bloqueen.

    Esta opción está deshabilitada de forma predeterminada.

## Configuración de eventos

En esta pestaña, puede configurar el registro de eventos y las notificaciones de eventos. Los eventos se organizan por nivel de importancia en las siguientes secciones de la pestaña **Configuración de eventos**:

- **Error funcional**
- **Advertencia**
- **Información**

Cada sección contiene una lista con los distintos tipos de eventos y, junto a ellos, la cantidad de días por los que cada evento se deja almacenado, por defecto, en el Servidor de administración. Cuando hace clic en un tipo de evento, puede especificar el registro de eventos y las notificaciones relativas a los eventos seleccionados en la lista. De forma predeterminada, la configuración de notificación común especificada para todo el Servidor de administración se usa para todos los tipos de eventos. Si lo necesita, puede modificar ajustes puntuales para los tipos de eventos que requieran cambios.

Por ejemplo, en la sección **Advertencia**, puede configurar el tipo de evento **Ocurrió un problema de seguridad**. Tales eventos pueden ocurrir, por ejemplo, cuando el espacio libre en el disco de un punto de distribución es inferior a 2 GB (se requieren al menos 4 GB para instalar aplicaciones y descargar actualizaciones de forma remota). Para configurar el evento **Ocurrió un problema de seguridad**, haga clic en este y especifique dónde almacenar los eventos ocurridos y cómo notificarlos.

Si el Agente de red detectó un problema de seguridad, puede administrar este problema utilizando la configuración de un dispositivo administrado.

## Configuración de la aplicación

## Configuración

En la sección **Configuración**, puede configurar la directiva del Agente de red:

- **Distribuir archivos solo a través de los puntos de distribución**

  Si se habilita esta opción, los Agentes de red en los dispositivos administrados recuperarán las actualizaciones solo de los puntos de distribución.

  Si se deshabilita esta opción, los Agentes de red en los dispositivos administrados recuperarán las actualizaciones de los puntos de distribución o del Servidor de administración.

  Tenga en cuenta que las aplicaciones de seguridad en los dispositivos administrados recuperan las actualizaciones del conjunto de origen de la tarea de actualización para cada aplicación de seguridad. Si habilita la opción **Distribuir archivos solo a través de los puntos de distribución**, asegúrese de que Kaspersky Security Center esté configurado como origen de actualización en las tareas de actualización.

  Esta opción está deshabilitada de forma predeterminada.

- **Tamaño máximo de la cola de eventos, en MB**

  En este campo se puede especificar el espacio máximo que puede ocupar una cola de evento en la unidad.

  El valor predeterminado es de 2 megabytes (MB).

- **La aplicación podrá obtener información adicional sobre la directiva en el dispositivo**

  La aplicación de seguridad de un dispositivo administrado (por ejemplo, Kaspersky Endpoint Security para Windows) recibe, del Agente de red instalado en el mismo dispositivo, información sobre la directiva que para ella se ha aplicado. Si lo desea, puede ver esta información en la interfaz de la aplicación de seguridad.

  El Agente de red le brinda los siguientes datos a la aplicación:

  - Hora en que la directiva se entregó en el dispositivo administrado.
  - Nombre de la directiva activa que se encontraba vigente cuando la directiva se entregó en el dispositivo administrado.
  - Nombre de la directiva fuera de la oficina que se encontraba vigente cuando la directiva se entregó en el dispositivo administrado (no disponible en el Agente de red para Linux).
  - Nombre y ruta completa al grupo de administración en el que se encontraba el dispositivo administrado cuando la directiva se entregó en el dispositivo administrado.
  - Lista de perfiles de directivas activas que se encontraban vigentes cuando la directiva se entregó en el dispositivo administrado, con sus nombres y prioridades.

  Puede utilizar esta información para solucionar problemas o verificar que la directiva aplicada al dispositivo sea la esperada. Esta opción está deshabilitada de forma predeterminada.

- **Evitar que el servicio del Agente de red se detenga o se elimine sin autorización e impedir cambios en su configuración**

  Cuando esta opción está habilitada, una vez que el Agente de red se encuentre instalado en un dispositivo administrado, no se lo podrá eliminar ni reconfigurar a menos que se tengan los privilegios necesarios. El servicio del Agente de red no se podrá detener. Esta opción no tiene efecto en los controladores de dominio.

  Habilite esta opción para proteger el Agente de red en estaciones de trabajo operadas con derechos de administrador local.

  Esta opción está deshabilitada de forma predeterminada.

- **Utilizar contraseña de desinstalación**

  Si activa esta opción y hace clic en el botón **Modificar**, podrá especificar la contraseña para la utilidad klmover y la desinstalación remota del Agente de red.

  Esta opción está deshabilitada de forma predeterminada.

## Repositorios

En la sección **Repositorios**, puede seleccionar los tipos de objetos sobre los que el Agente de red enviará detalles al Servidor de administración. La directiva del Agente de red podría impedirle modificar algunos ajustes de esta sección.

- **Detalles de las aplicaciones instaladas**

  Si se habilita esta opción, la información sobre las aplicaciones instaladas en los dispositivos cliente se enviará al Servidor de administración.

  Esta opción está activada de forma predeterminada.

- **Incluir información sobre parches**

  Se enviará información al Servidor de administración sobre los parches de las aplicaciones instaladas en los dispositivos clientes. Si habilita esta opción, podría aumentar la carga del Servidor de administración y del sistema de administración de bases de datos (DBMS). También podría aumentar el volumen de la base de datos.

  Esta opción está activada de forma predeterminada. Está disponible solo para Windows.

- **Detalles de las actualizaciones de Windows Update**

  Si esta opción está habilitada, se enviará información al Servidor de administración sobre las actualizaciones de Microsoft Windows Update que deban instalarse en los dispositivos cliente.

  Aunque deshabilite esta opción, ocasionalmente encontrará actualizaciones en la sección **Actualizaciones disponibles** de las propiedades de un dispositivo. Esto podría suceder, por ejemplo, cuando los dispositivos de la organización tengan vulnerabilidades que puedan repararse con esas actualizaciones.

  Esta opción está activada de forma predeterminada. Está disponible solo para Windows.

  La información sobre las actualizaciones opcionales de Microsoft Windows no se envía al Servidor de administración.

- Detalles de vulnerabilidades de software y actualizaciones correspondientes

  Si esta opción está habilitada, se enviará información al Servidor de administración sobre las vulnerabilidades que se detecten en las aplicaciones de terceros instaladas en los dispositivos administrados (incluidas las aplicaciones de Microsoft) y sobre las actualizaciones disponibles para reparar vulnerabilidades en aplicaciones de terceros (excluidas, en este caso, las aplicaciones de Microsoft).

  Si habilita la opción **Detalles de las vulnerabilidades de software y las actualizaciones correspondientes**, aumentarán la carga en la red, la carga en el disco del Servidor de administración y el uso de recursos del Agente de red.

  Esta opción está activada de forma predeterminada. Está disponible solo para Windows.

  Para administrar las actualizaciones de software de Microsoft, use la opción **Detalles de las actualizaciones de Windows Update**.

- Detalles del registro de hardware

  Cuando el Agente de red está instalado en un dispositivo, envía información acerca del hardware de dicho dispositivo al Servidor de administración. Puede ver los detalles del hardware en las propiedades del dispositivo.

  Asegúrese de que la utilidad lshw esté instalada en los dispositivos Linux desde los que desea obtener detalles del hardware. Los detalles de hardware obtenidos de las máquinas virtuales pueden estar incompletos según el hipervisor que se utilice.

## Actualizaciones y vulnerabilidades de software

En la sección **Actualizaciones y vulnerabilidades de software** puede configurar la búsqueda y distribución de actualizaciones de Windows, como también activar la búsqueda de vulnerabilidades en archivos ejecutables:

- **Usar el Servidor de administración como servidor WSUS**

  Si se habilita esta opción, las actualizaciones de Windows se descargarán al Servidor de administración. El Servidor de administración proporciona las actualizaciones descargadas a Windows Update en los dispositivos cliente en modo centralizado, mediante Agentes de red.

  Si se deshabilita esta opción, el Servidor de administración no se utilizará para descargar las actualizaciones de Windows. En tal caso, los dispositivos cliente reciben las actualizaciones de Windows por sus propios medios.

  Esta opción está deshabilitada de forma predeterminada.

- Puede limitar las actualizaciones de Windows que los usuarios pueden instalar manualmente en sus dispositivos mediante Windows Update.

  Si selecciona una nueva opción en **Permitir que los usuarios administren la instalación de actualizaciones de Windows Update** luego de que Windows Update encuentre actualizaciones para un dispositivo con Windows 10, la nueva opción no entrará en vigor sino hasta que se instalen esas actualizaciones.

  Seleccione un elemento en la lista desplegable:

  - **Permitir a los usuarios instalar todas las actualizaciones de Windows Update aplicables**

    Los usuarios podrán instalar cualquier actualización de Microsoft Windows Update que resulte adecuada para sus dispositivos.

    Seleccione esta opción si prefiere no interferir en la instalación de actualizaciones.

    Cuando un usuario instala actualizaciones de Microsoft Windows Update manualmente, puede suceder que los archivos de actualización se descarguen de los servidores de Microsoft y no del Servidor de administración. Esto puede ocurrir si el Servidor de administración no ha descargado aún esas actualizaciones. Descargar actualizaciones de los servidores de Microsoft genera tráfico adicional.

  - **Permitir a los usuarios instalar solo actualizaciones aprobadas de Windows Update**

Los usuarios podrán instalar cualquier actualización de Microsoft Windows Update que resulte adecuada para sus dispositivos y que usted haya aprobado.

Podría suceder, por ejemplo, que primero quiera instalar las actualizaciones en un entorno de prueba para verificar que no interfieran con el funcionamiento de los dispositivos, y solo entonces, en caso de no detectarse problemas, permitir que las actualizaciones aprobadas se instalen en los dispositivos cliente.

Cuando un usuario instala actualizaciones de Microsoft Windows Update manualmente, puede suceder que los archivos de actualización se descarguen de los servidores de Microsoft y no del Servidor de administración. Esto puede ocurrir si el Servidor de administración no ha descargado aún esas actualizaciones. Descargar actualizaciones de los servidores de Microsoft genera tráfico adicional.

- **No permitir que los usuarios instalen actualizaciones de Windows Update**

  Los usuarios no podrán instalar manualmente ninguna actualización de Microsoft Windows Update en sus dispositivos. Toda actualización que resulte adecuada se instalará respetando la configuración que usted defina.

  Seleccione esta opción si desea administrar la instalación de actualizaciones en forma central.

  Podría utilizar esta opción, por ejemplo, para optimizar el cronograma de instalación de actualizaciones y evitar sobrecargas en la red. Puede programar la instalación para que se lleve a cabo fuera del horario laboral a fin de no interferir con la productividad de los usuarios.

- Utilice el grupo de opciones **Modo de búsqueda de Windows Update** para seleccionar el modo de búsqueda de actualizaciones:

  - **Activo**

    Si selecciona esta opción, el Servidor de administración (asistido por el Agente de red) hará que el Agente de Windows Update del dispositivo cliente realice una solicitud al origen de actualizaciones (los servidores de Windows Update o WSUS). Tras ello, el Agente de red transmitirá al Servidor de administración la información que reciba del Agente de Windows Update.

    Esta opción solo tiene efecto si la tarea *Buscar vulnerabilidades y actualizaciones requeridas* tiene habilitada la opción **Conectarse al servidor de actualizaciones para actualizar los datos**.

    Esta opción está seleccionada de forma predeterminada.

  - **Pasivo**

    Si selecciona esta opción, el Agente de red se comunicará periódicamente con el Servidor de administración para enviarle información sobre las actualizaciones obtenidas durante la última sincronización entre el Agente de Windows Update y el origen de actualizaciones. Si el Agente de Windows Update no se sincroniza con un origen de actualizaciones, la información sobre actualizaciones del Servidor de administración se vuelve obsoleta.

    Seleccione esta opción si desea obtener actualizaciones de la caché del origen de actualizaciones.

  - **Deshabilitado**

    Si selecciona esta opción, el Servidor de administración no solicitará información sobre las actualizaciones.

    Seleccione esta opción si, por ejemplo, desea probar primero las actualizaciones en su dispositivo local.

- **Analizar los archivos ejecutables en busca de vulnerabilidades al iniciarlos**

  Si habilita esta opción, cuando se inicie un archivo ejecutable, se lo analizará en busca de vulnerabilidades.

  Esta opción está activada de forma predeterminada.

## Opciones de reinicio

En la sección **Opciones de reinicio**, puede indicar qué acción se llevará a cabo cuando se necesite reiniciar el sistema operativo de un dispositivo administrado para que una aplicación pueda instalarse, desinstalarse o utilizarse correctamente.

- **No reiniciar el sistema operativo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

- **Reiniciar el sistema operativo automáticamente si es necesario**

  Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

  Esta opción está seleccionada de forma predeterminada.

  - **Repetir la solicitud cada (min)**

    Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

    Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

    Si no habilita esta opción, la solicitud se mostrará una sola vez.

  - **Forzar reinicio después de (min)**

    Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

    Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

  - **Forzar el cierre de aplicaciones en sesiones bloqueadas**

Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

Esta opción está deshabilitada de forma predeterminada.

## Windows Desktop Sharing

En la sección **Windows Desktop Sharing**, puede activar y configurar la auditoría de las acciones del administrador que se realizan en un dispositivo remoto cuando se comparte el acceso al escritorio.

- **Habilitar auditoría**

  Habilite esta opción si desea auditar las operaciones que el administrador realice en el dispositivo remoto. Los registros de las acciones del administrador en el dispositivo remoto se computan:

  - En el registro de eventos del dispositivo remoto
  - en un archivo con la extensión syslog ubicado en la carpeta de instalación del Agente de red del dispositivo remoto
  - en la base de datos de eventos de Kaspersky Security Center

  La auditoría de las acciones del administrador está disponible cuando se cumplen las siguientes condiciones:

  - La licencia de Administración de vulnerabilidades y parches está en uso
  - El administrador tiene permiso para ejecutar el acceso compartido al escritorio del dispositivo remoto

  Si no necesita auditar las operaciones del administrador en el dispositivo remoto, no habilite esta opción.

  Esta opción está deshabilitada de forma predeterminada.

- **Máscaras de los archivos cuya lectura se debe supervisar**

  La lista contiene máscaras de archivos. Cuando la auditoría está habilitada, la aplicación monitorea los archivos de lectura del administrador que coinciden con las máscaras y guarda información sobre los archivos leídos. La lista está disponible si se ha marcado la casilla **Habilitar auditoría**. Puede editar máscaras de archivos y agregar máscaras nuevas a la lista. Cada máscara de archivo nueva se debe especificar en la lista en una línea nueva.

  De forma predeterminada, están especificadas las siguientes máscaras de archivos:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Máscaras de los archivos cuya modificación se debe supervisar**

  La lista contiene las máscaras de archivos en el dispositivo remoto. Cuando la auditoría está habilitada, la aplicación monitorea los cambios realizados por el administrador en los archivos que coinciden con las máscaras y guarda información sobre esas modificaciones. La lista está disponible si se ha marcado la casilla **Habilitar auditoría**. Puede editar máscaras de archivos y agregar máscaras nuevas a la lista. Cada máscara de archivo nueva se debe especificar en la lista en una línea nueva.

  De forma predeterminada, están especificadas las siguientes máscaras de archivos:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

## Administrar parches y actualizaciones

En la sección **Administrar parches y actualizaciones**, puede configurar la descarga y la distribución de actualizaciones, así como la instalación de parches en los dispositivos administrados:

- **Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes**

  Si esta opción está habilitada, los parches de Kaspersky con el estado de aprobación *Sin definir* se instalan automáticamente en los dispositivos administrados inmediatamente después de que se descargan de los servidores de actualizaciones.

  Si deshabilita esta opción, los parches de Kaspersky que se descarguen y que tengan el estado *Sin definir* se instalarán únicamente si cambia su estado a *Aprobada*.

  Esta opción está activada de forma predeterminada.

- **Descargar actualizaciones y bases de datos antivirus del Servidor de administración con anticipación (recomendado)**

  Si esta opción está habilitada, las actualizaciones se descargan utilizando el modelo sin conexión. Cuando el Servidor de administración recibe actualizaciones, notifica al Agente de red (en los dispositivos donde está instalado) las actualizaciones que serán necesarias para las aplicaciones administradas. Cuando el Agente de red recibe la información sobre las actualizaciones, descarga por anticipado los archivos relevantes desde el Servidor de administración. En la primera conexión con un Agente de red, el Servidor de administración inicia una descarga de actualizaciones. Después de que Agente de red descarga todas las actualizaciones a un dispositivo cliente, las actualizaciones quedan disponibles para las aplicaciones en ese dispositivo.

  Cuando una aplicación administrada de un dispositivo cliente intenta acceder al Agente de red para descargar actualizaciones, el Agente de red comprueba si tiene todas las actualizaciones necesarias. Si las actualizaciones se reciben desde el Servidor de administración no más de 25 horas antes de que la aplicación administrada las solicite, el Agente de red no se conecta al Servidor de administración, sino que proporciona actualizaciones desde el caché local a la aplicación administrada. Es posible que la conexión con el Servidor de administración no se establezca cuando el Agente de red proporciona actualizaciones para las aplicaciones en los dispositivos cliente, pero no se requiere conexión para la actualización.

  Deshabilite esta opción si prefiere no utilizar el modelo de descarga de actualizaciones sin conexión. Las actualizaciones se distribuirán siguiendo la programación de la tarea de descarga de actualizaciones.

  Esta opción está activada de forma predeterminada.

## Conectividad

La sección **Conectividad** incluye tres subsecciones:

- **Red**
- **Perfiles de conexión**
- **Programación de conexiones**

En la subsección **Red**, puede configurar la conexión al Servidor de administración, habilitar el uso de un puerto UDP y especificar el número de ese puerto UDP.

- En el grupo de configuraciones **Conexión con el Servidor de administración**, puede configurar la conexión con el Servidor de administración y especificar el intervalo de tiempo para la sincronización entre dispositivos cliente y el Servidor de administración.

  - **Intervalo de sincronización (min)**

    El Agente de red se encarga de sincronizar el dispositivo administrado con el Servidor de administración. Recomendamos que el intervalo de sincronización (también llamado latido) se fije en 15 minutos por cada 10 000 dispositivos administrados.

    Si define un intervalo de sincronización inferior a 15 minutos, la sincronización se realizará cada 15 minutos. Si el intervalo de sincronización está configurado en 15 minutos o más, la sincronización se realiza en el intervalo de sincronización especificado.

  - **Comprimir tráfico de red**

    Si esta opción está habilitada, se reducirá el volumen de datos transferido. En consecuencia, el Agente de red podrá transmitir información a mayor velocidad y el Servidor de administración deberá soportar menos carga.

    El uso de la CPU del equipo cliente podría aumentar.

    Esta casilla está activada de manera predeterminada.

  - **Abrir puertos del Agente de red en el Firewall de Microsoft Windows**

    Cuando se habilita esta opción, se agregan los puertos que el Agente de red y el Servidor de administración necesitan para funcionar a la lista de exclusiones del Firewall de Microsoft Windows.

    Esta opción está activada de forma predeterminada.

  - **Usar conexión SSL**

    Si se habilita esta opción, la conexión al Servidor de administración se establecerá a través de un puerto seguro utilizando el protocolo SSL.

    Esta opción está activada de forma predeterminada.

  - **Utilizar la puerta de enlace de conexión del punto de distribución (si está disponible) con la configuración de conexión predeterminada**

    Si esta opción está habilitada, la puerta de enlace de conexión del punto de distribución se usará con la configuración especificada en las propiedades del grupo de administración.

    Esta opción está activada de forma predeterminada.

- **Usar puerto UDP**

Si necesita que el Agente de red se conecte al Servidor de administración a través de un puerto UDP, habilite la opción **Usar puerto UDP** y especifique un **número de puerto UDP**. Esta opción está activada de forma predeterminada. El puerto UDP predeterminado para conectarse al Servidor de administración es 15000.

- **Número de puerto UDP**

  En este campo, puede indicar el número del puerto UDP. El número de puerto predeterminado es 15000.

  El sistema decimal se usa para los registros.

  En dispositivos cliente con Windows XP Service Pack 2, el puerto UDP 15000 estará bloqueado por el firewall integrado. Deberá abrir el puerto manualmente.

- **Utilizar el punto de distribución para forzar la conexión con el Servidor de administración**

  Seleccione esta opción si seleccionó **Utilizar este punto de distribución como servidor push** en la ventana de configuración del punto de distribución. De lo contrario, el punto de distribución no funcionará como un servidor push.

En la subsección **Perfiles de conexión**, puede especificar la configuración de las ubicaciones de red y habilitar el modo fuera de la oficina cuando el Servidor de administración no esté disponible:

- Configuración de ubicación de red

  La configuración de una ubicación de red define las características de la red con la cual está conectado el dispositivo cliente y especifica las reglas que hacen que el Agente de red cambie de un perfil de conexión de Servidor de administración a otro en respuesta a un cambio en las características de la red.

- Perfiles de conexión al Servidor de administración

  En esta sección, puede ver y crear los perfiles que rigen la conexión entre el Agente de red y el Servidor de administración. Desde aquí también puede crear reglas para que el Agente de red cambie a un Servidor de administración diferente cuando ocurren los siguientes eventos:

  - Cuando el dispositivo cliente se conecta a otra red local
  - Cuando el dispositivo pierde la conexión con la red local de la organización
  - Cuando se modifican la dirección de la puerta de enlace de conexión o la dirección del servidor DNS

  Los perfiles de conexión solo son compatibles con dispositivos que ejecutan Windows y MacOS.

- Habilitar el modo de fuera de la oficina cuando el Servidor de administración no esté disponible

  Si se habilita esta opción, en caso de que se establezca la conexión mediante este perfil, las aplicaciones instaladas en el dispositivo cliente utilizarán perfiles de directiva para dispositivos en modo fuera de la oficina, así como directivas para fuera de la oficina. Si no hay una directiva fuera de la oficina definida para la aplicación, se utilizará la directiva activa.

  Si se deshabilita esta opción, las aplicaciones utilizarán directivas activas.

  Esta opción está deshabilitada de forma predeterminada.

En la subsección **Programación de conexiones**, puede especificar los intervalos de tiempo durante los cuales el Agente de red enviará datos al Servidor de administración:

- Establecer conexión cuando sea necesario

  Si se selecciona esta opción, la conexión se establece cuando el Agente de red debe enviar datos al Servidor de administración.

  Esta opción está seleccionada de forma predeterminada.

- Establecer conexión en los intervalos que especifique

  Si se selecciona esta opción, el Agente de red se conecta al Servidor de administración a una hora especificada. Puede agregar varios períodos de conexión.

## Sondeo de red con puntos de distribución

En la sección **Sondeo de red con puntos de distribución**, puede configurar el sondeo automático de la red. Puede utilizar las siguientes opciones para habilitar el sondeo y definir una frecuencia de sondeo:

- **Red de Windows**

  Si se habilita esta opción, el Servidor de administración sondeará automáticamente la red de acuerdo con la programación que configuró al hacer clic en los enlaces **Establecer programación de sondeo rápido** y **Establecer programación de sondeo completo**.

  Si esta opción está deshabilitada, el Servidor de administración sondeará la red con la frecuencia indicada en el campo **Frecuencia de sondeos de la red (min)**.

  El intervalo de detección de dispositivos para las versiones de Agente de red anteriores a la 10.2 se puede configurar en los campos **Frecuencia de sondeos de dominios de Windows (min)** (para el sondeo rápido de redes Windows) y **Frecuencia de sondeos de la red (min)** (para el sondeo completo de redes Windows).

  Esta opción está deshabilitada de forma predeterminada.

- **Zeroconf**

  Si esta opción está habilitada, el punto de distribución automáticamente sondea la red con dispositivos IPv6 mediante el uso de las redes de configuración cero (también denominadas *Zeroconf*). En este caso, el sondeo de rangos de IP habilitados se ignora, porque el punto de distribución sondea toda la red.

  Para empezar a usar Zeroconf, se deben cumplir las siguientes condiciones:

  - El punto de distribución debe ejecutar Linux.
  - Debe instalar la utilidad avahi-browse en el punto de distribución.

  Si esta opción está habilitada, el punto de distribución no sondea las redes con dispositivos IPv6.

  Esta opción está deshabilitada de forma predeterminada.

- Intervalos IP

  Si se habilita esta opción, el punto de distribución sondeará automáticamente los intervalos IP siguiendo la programación que se haya configurado tras hacer clic en el botón **Configurar programación de sondeos**.

  Si esta opción no está habilitada, el punto de distribución no hará sondeos de intervalos IP.

  La frecuencia de sondeo de rangos IP para las versiones del Agente de red anteriores a la versión 10.2 se puede configurar en el campo **Intervalo de sondeo (min)**. El campo estará disponible si se habilita la opción.

  Esta opción está deshabilitada de forma predeterminada.

- Controladores de dominio

  Si se habilita esta opción, el Servidor de administración sondeará automáticamente Active Directory de acuerdo con la programación que configuró al hacer clic en el vínculo **Configurar programación de sondeos**.

  Si se deshabilita esta opción, el Servidor de administración no sondeará Active Directory.

  La frecuencia de sondeo de Active Directory para las versiones del Agente de red anteriores a la versión 10.2 se puede configurar en el campo **Intervalo de sondeo (min)**. El campo estará disponible si se habilita esta opción.

  Esta opción está deshabilitada de forma predeterminada.

  Si se habilita esta opción, el punto de distribución sondeará automáticamente los controladores de dominio de acuerdo con la programación que configuró al hacer clic en el botón **Configurar programación de sondeos**.

  Si esta opción no está habilitada, el punto de distribución no hará sondeos de controladores de dominio.

  La frecuencia de sondeo de controladores de dominio para las versiones del Agente de red anteriores a la versión 10.2 se puede configurar en el campo **Intervalo de sondeo (min)**. El campo estará disponible si se habilita esta opción.

  Esta opción está deshabilitada de forma predeterminada.

## Configuración de red para puntos de distribución

Si sus puntos de distribución utilizan un servidor proxy al conectarse a Internet, en la sección **Configuración de red para puntos de distribución**, puede especificar la siguiente configuración:

- **Usar servidor proxy**
- **Dirección**
- **Número de puerto**

- No usar el servidor proxy para direcciones locales

  Si habilita esta opción, no se usará un servidor proxy para establecer conexión con los dispositivos de la red local.

  Esta opción está deshabilitada de forma predeterminada.

- Autenticación del servidor proxy

  Si se selecciona esta casilla, en los campos de entrada se podrán especificar las credenciales para la autenticación del servidor proxy.

  Esta casilla no está marcada de manera predeterminada.

- **Nombre de usuario**

- **Contraseña**

## Proxy de KSN (puntos de distribución)

En la sección **Proxy de KSN (puntos de distribución)**, puede hacer que la aplicación utilice el punto de distribución para reenviar las solicitudes para Kaspersky Security Network (KSN) de los dispositivos administrados:

- Habilitar el proxy de KSN en el lado del punto de distribución

  El servicio de proxy de KSN se ejecuta en el dispositivo que se utiliza como punto de distribución. Utilice esta función para redistribuir y optimizar el tráfico de la red.

  El punto de distribución enviará a Kaspersky las estadísticas de KSN que se enumeran en la declaración de Kaspersky Security Network. De forma predeterminada, la declaración de KSN se encuentra en %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

  Esta opción está deshabilitada de forma predeterminada. Esta opción solo se habilita si las opciones **Usar Servidor de administración como servidor proxy** y **Acepto utilizar Kaspersky Security Network** están habilitadas en la ventana de propiedades del Servidor de administración.

  Puede asignar un nodo de un clúster activo-pasivo a un punto de distribución y habilitar el servidor proxy de KSN en ese nodo.

- Transmitir las solicitudes para KSN al Servidor de administración

  El punto de distribución envía las solicitudes KSN desde los dispositivos administrados al Servidor de administración.

  Esta opción está activada de forma predeterminada.

- **Acceder a KSN Cloud/KPSN directamente a través de Internet**

  El punto de distribución envía las solicitudes KSN desde los dispositivos administrados a KSN Cloud o a KPSN. Las solicitudes de KSN generadas en el punto de distribución mismo también se envían directamente a la nube de KSN Cloud o a KPSN.

  Los puntos de distribución que tienen instalado el Agente de red versión 11 (o versiones anteriores) no pueden acceder a KPSN directamente. Si desea reconfigurar los puntos de distribución para enviar solicitudes de KSN a KPSN, habilite la opción **Reenviar solicitudes KSN al Servidor de administración** para cada punto de distribución.

  Los puntos de distribución que tienen instalado el Agente de red versión 12 (o una posterior) pueden acceder a KPSN directamente.

- **Puerto**

  El número del puerto de TCP que los dispositivos administrados utilizarán para conectarse al Servidor proxy de KSN. El número de puerto predeterminado es 13111.

- **Puerto UDP**

  Si necesita que el Agente de red se conecte al Servidor de administración a través de un puerto UDP, habilite la opción **Usar puerto UDP** y especifique un **número de puerto UDP**. Esta opción está activada de forma predeterminada. El puerto UDP predeterminado para conectarse al Servidor de administración es 15000.

## Actualizaciones (puntos de distribución)

En la sección **Actualizaciones (puntos de distribución)**, puede habilitar la función de descarga de archivos diff, para que los puntos de distribución reciban actualizaciones en forma de archivos diff desde los servidores de actualización de Kaspersky.

## Administración de cuenta local (solo Linux)

La sección **Administración de cuenta local (solo Linux)** incluye tres subsecciones:

- **Administración de certificados de usuario**
- **Agregar o editar grupos de administradores locales vigentes**
- **Carga de archivo de referencia para proteger frente a la modificación del archivo de sudoers en el dispositivo del usuario**

En la subsección **Administración de certificados de usuario**, puede especificar qué certificados raíz instalar. Estos certificados se pueden utilizar, por ejemplo, para verificar la autenticidad de sitios web o servidores web.

- **Instalar certificados raíz**

  Si esta opción está habilitada, los certificados agregados a la tabla se instalarán en los dispositivos especificados.

  Si esta opción está deshabilitada, no se instalarán certificados en los dispositivos especificados.

  Esta opción está deshabilitada de forma predeterminada.

- **Agregar**

  Al hacer clic en este botón, se abre una ventana en la que puede agregar un certificado.

  El certificado debe ser inferior a 10 MB.

  Kaspersky Security Center admite certificados con extensiones CER, CRT, CERT, PEM y KEY.

En la subsección **Agregar o editar grupos de administradores locales vigentes**, puede administrar grupos de administradores locales. Estos grupos se utilizan, por ejemplo, al revocar los derechos de administrador local. También puede consultar la lista de cuentas de usuarios con privilegios mediante **Informe sobre usuarios privilegiados en el dispositivo (solo Linux)**.

- **Agregar**

  Al hacer clic en este botón, se abre una ventana en la que puede agregar un grupo de administradores locales.

- **Editar**

  Al hacer clic en este botón, se abre una ventana en la que puede editar el grupo de administradores locales.

  Este botón está disponible si se selecciona la casilla junto al grupo de administradores locales.

- **Eliminar**

  Al hacer clic en este botón, se elimina de la tabla el grupo de administradores locales seleccionado.

  Este botón está disponible si se selecciona la casilla junto al grupo de administradores locales.

En la subsección **Carga de archivo de referencia para proteger frente a la modificación del archivo de sudoers en el dispositivo del usuario**, puede configurar el control del archivo sudoers. Los grupos con privilegios y los usuarios del dispositivo se definen mediante el archivo sudoers en el dispositivo. El archivo sudoers se encuentra en `/etc/sudoers`. Puede cargar un archivo sudoers de referencia para proteger el archivo sudoers contra cambios. Esto evitará cambios no deseados en el archivo sudoers.

Un archivo sudoers de referencia no válido puede hacer que el dispositivo del usuario no funcione correctamente.

- **Controlar archivo de sudoers**

  Si esta opción está habilitada, el archivo sudoers será reemplazado por el archivo sudoers de referencia actual.

  Si esta opción está deshabilitada, el archivo sudoers permanecerá sin cambios.

  Esta opción está deshabilitada de forma predeterminada.

- **Archivo de referencia de sudoers**

  Este campo muestra el nombre del archivo sudoers de referencia cargado.

- **Cargar**

  Al hacer clic en este botón, se abre una ventana en la que puede cargar un archivo sudoers de referencia.

- **Archivo de referencia de sudoers actual**

  Al hacer clic en este botón, se muestra el contenido del archivo sudoers actual.

### Historial de revisiones

En esta pestaña, puede ver la lista de revisiones de la directiva y revertir los cambios realizados en la directiva, si es necesario.

## Comparación de la configuración de la directiva del Agente de red por sistemas operativos

La siguiente tabla muestra qué configuraciones de directiva del Agente de red puede usar en la Consola de administración y en la Kaspersky Security Center Web Console para configurar el Agente de red con un sistema operativo específico.

Configuración de la directiva del Agente de red: comparación por sistemas operativos

| Sección de la directiva | Windows | macOS | Linux |
|---|---|---|---|
| General | ✓ | ✓ | ✓ |
| Configuración de eventos | ✓ | ✓ | ✓ |

| Sección de la directiva | Windows | macOS | Linux |
|---|---|---|---|
| Configuración | ✓ | ✓ | ✓<br>Están disponibles las siguientes opciones:<br>• **Distribuir archivos solo a través de los puntos de distribución**<br>• **Tamaño máximo de la cola de eventos, en MB**<br>• **La aplicación podrá obtener información adicional sobre la directiva en el dispositivo** |
| Repositorios | ✓ | ✓<br>La opción **Detalles del Registro de hardware** está disponible. | ✓<br>Están disponibles las siguientes opciones:<br>• **Detalles de las aplicaciones instaladas**<br>• **Detalles del registro de hardware** |
| Actualizaciones y vulnerabilidades de software | ✓ | — | — |
| Opciones de reinicio | ✓ | — | — |
| Windows Desktop Sharing | ✓ | — | — |
| Administrar parches y actualizaciones | ✓ | — | — |
| Conectividad → Red | ✓ | ✓ | ✓<br>Excepto la opción **Abrir puertos del Agente de red en el Firewall de Microsoft Windows**. |
| Conectividad → Perfiles de conexión | ✓ | ✓ | — |
| Conectividad → Programación de conexiones | ✓ | ✓ | ✓ |
| Sondeo de red con puntos de distribución | ✓<br>Solo están disponibles las opciones **Red de Windows**, **Intervalos IP** y **Controladores de dominio**. | — | ✓<br>Están disponibles las siguientes opciones:<br>• **Zeroconf**<br>• **Intervalos IP**<br>• **Controladores de dominio** |
| Configuración de red para puntos de distribución | ✓ | ✓ | ✓ |
| Proxy de KSN (puntos de distribución) | ✓ | — | ✓ |
| Actualizaciones (puntos de distribución) | ✓ | — | ✓ |
| Historial de revisiones | ✓ | ✓ | ✓ |

# Habilitar y deshabilitar el modo de bajo consumo de recursos para el Agente de red

El modo de bajo consumo de recursos permite limitar el uso de RAM del Agente de red instalado en el dispositivo cliente. El modo de bajo consumo de recursos está deshabilitado de manera predeterminada.

En el modo de bajo consumo de recursos, las siguientes prestaciones no están disponibles:

- El Agente de red no se puede designar como punto de distribución (ya sea de forma manual o automática).
- El Agente de red no registra información sobre el estado del Agente de red en un archivo de texto separado.
- El Agente de red no permite utilizar el modelo sin conexión de descarga de actualizaciones.
- Los siguientes componentes y procesos se deshabilitan:
  - Obtención de información sobre actualizaciones y vulnerabilidades de terceros.
  - Ejecución del proxy de KSN en el punto de distribución.
  - Carga de actualizaciones al repositorio del punto de distribución.
  - Anulación del bloqueo del servidor DNS.
  - Información sobre el espacio libre en disco.

Los componentes y procesos reanudan su funcionamiento cuando se deshabilita el modo de bajo consumo de recursos.

*Para habilitar el modo de bajo consumo de recursos, haga lo siguiente:*

1. Ejecute el siguiente comando en la línea de comandos del dispositivo cliente:

   ```
   C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. Reinicie el Agente de red.
3. Para verificar si el modo de bajo consumo de recursos está habilitado, en Windows, abra **Visor de eventos** y luego seleccione **Registros de aplicaciones y servicios → Registro de eventos de Kaspersky**.

   Asegúrese de que el registro contenga eventos como **Agente de red de Kaspersky Security Center está funcionando en modo de bajo consumo de recursos**.

El modo de bajo consumo de recursos queda habilitado.

*Para deshabilitar el modo de bajo consumo de recursos, haga lo siguiente:*

1. Ejecute el siguiente comando en la línea de comandos del dispositivo cliente:

   ```
   C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. Reinicie el Agente de red.
3. Para verificar si el modo de bajo consumo de recursos está deshabilitado, en Windows, abra **Visor de eventos** y luego seleccione **Registros de aplicaciones y servicios → Registro de eventos de Kaspersky**.

   Asegúrese de que el último evento de klnagent no contenga el mensaje **Agente de red de Kaspersky Security Center está funcionando en modo de bajo consumo de recursos**.

El modo de bajo consumo de recursos queda deshabilitado.

También puede habilitar el modo de bajo consumo de recursos de forma remota mediante la tarea *Ejecución remota de scripts*.

# Configuración manual de la directiva de Kaspersky Endpoint Security

Esta sección proporciona recomendaciones sobre cómo configurar la directiva de Kaspersky Endpoint Security. Puede realizar la configuración en la ventana de propiedades de la directiva. Cuando edite una configuración, haga clic en el icono de candado que hay a la derecha del grupo de configuraciones correspondiente para aplicar los valores especificados a una estación de trabajo.

## Configurar Kaspersky Security Network

Kaspersky Security Network (KSN) es la infraestructura de servicios en la nube que contiene información sobre la reputación de archivos, recursos web y software. Kaspersky Security Network permite que Kaspersky Endpoint Security para Windows responda más rápido a los distintos tipos de amenazas, mejora el rendimiento de los componentes de protección y reduce la probabilidad de falsos positivos. Para obtener más información acerca de Kaspersky Security Network, consulte la Ayuda de Kaspersky Endpoint Security para Windows.

*Para definir los ajustes recomendados para KSN:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en la directiva de Kaspersky Endpoint Security para Windows.

   Se abrirá la ventana de propiedades de la directiva seleccionada.
3. En las propiedades de la directiva, vaya a **Configuración de la aplicación** → **Protección avanzada contra amenazas** → **Kaspersky Security Network**.
4. Asegúrese de que la opción **Kaspersky Security Network** esté activa. Esta función ayuda a redistribuir y optimizar el tráfico de la red.

   Si utiliza Managed Detection and Response, debe activar la opción **Kaspersky Security Network** para el punto de distribución y activar el modo de KSN extendido.
5. Habilite el uso de servidores KSN si el servicio del proxy de KSN no está disponible. Los servidores de KSN pueden estar alojados en la infraestructura de Kaspersky (este es el caso cuando se utiliza KSN) o en la infraestructura de un tercero (cuando se utiliza KPSN).
6. Haga clic en **Aceptar**.

Se guardan los ajustes recomendados para KSN.

## Comprobar la lista de las redes protegidas por Firewall.

Asegúrese de que el Firewall de Kaspersky Endpoint Security para Windows proteja todas sus redes. De forma predeterminada, el Firewall protege las redes con los siguientes tipos de conexión:

- **Red pública**. Las aplicaciones de seguridad, los firewalls o los filtros no protegen los dispositivos de dicha red.
- **Red local**. El acceso a archivos e impresoras está restringido para dispositivos en esta red.
- **Red de confianza**. Los dispositivos en dicha red están protegidos contra ataques y accesos no autorizados a archivos y datos.

Si ha configurado una red personalizada, asegúrese de que el Firewall la proteja. Para ello, consulte la lista de redes en las propiedades de la directiva de Kaspersky Endpoint Security for Windows. La lista puede no contener todas las redes.

Para obtener más información acerca de Firewall, consulte la Ayuda de Kaspersky Endpoint Security para Windows.

*Para revisar la lista de redes:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en la directiva de Kaspersky Endpoint Security para Windows.

   Se abrirá la ventana de propiedades de la directiva seleccionada.
3. En las propiedades de la directiva, vaya a **Configuración de la aplicación** → **Protección básica contra amenazas** → **Firewall**.
4. En **Redes disponibles**, haga clic en el vínculo **Configuración de red**.

   Se abrirá la ventana **Conexiones de red**. La ventana contiene la lista de redes.
5. Si falta una red en la lista, agréguela.

## Desactivar el análisis de los dispositivos de red

Si permite que Kaspersky Endpoint Security para Windows analice las unidades de almacenamiento compartidas en red, estas pueden verse sometidas a una carga excesiva. Es preferible realizar análisis indirectos en los servidores de archivos.

Puede desactivar el análisis de unidades de red en las propiedades de la directiva de Kaspersky Endpoint Security para Windows. Para consultar la descripción de estas propiedades de directiva, consulte la Ayuda de Kaspersky Endpoint Security para Windows.

*Para deshabilitar el análisis de unidades de red:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en la directiva de Kaspersky Endpoint Security para Windows.

   Se abrirá la ventana de propiedades de la directiva seleccionada.

3. En las propiedades de la directiva, vaya a **Configuración de la aplicación → Protección básica contra amenazas → Protección contra amenazas de archivo**.

4. En **Alcance de la protección**, desactive la opción **Todas las unidades de red**.

5. Haga clic en **Aceptar**.

Se deshabilita el análisis de unidades de red.

## Excluir detalles de software de la memoria del Servidor de administración

Recomendamos que el Servidor de administración no guarde información sobre los módulos de software que se inician en los dispositivos de red. De esta manera, se evita que se desborde la memoria del Servidor de administración.

Puede desactivar el almacenamiento de esta información en las propiedades de la directiva de Kaspersky Endpoint Security para Windows.

*Para evitar que se guarde información sobre los módulos de software instalados:*

1. En el menú principal, vaya a **Activos (dispositivos) → Directivas y perfiles**.

2. Haga clic en la directiva de Kaspersky Endpoint Security para Windows.

   Se abrirá la ventana de propiedades de la directiva seleccionada.

3. En las propiedades de la directiva, vaya a **Configuración de la aplicación → Configuración general → Informes y repositorios**.

4. En **Transferencia de datos al Servidor de administración**, si aún está activa en la directiva de nivel superior, desmarque la casilla **Acerca de las aplicaciones iniciadas**.

   Cuando esta casilla está seleccionada, la base de datos del Servidor de administración guarda la información acerca de todas las versiones de todos los módulos de software en los dispositivos en red. Esta información puede requerir una cantidad significativa de espacio en disco en la base de datos de Kaspersky Security Center (docenas de gigabytes).

La base de datos del Servidor de administración ya no contendrá información sobre los módulos de software instalados.

## Configurar el acceso a la interfaz de Kaspersky Endpoint Security para Windows en las estaciones de trabajo

Si la protección contra amenazas en la red de la organización se debe administrar en modo centralizado a través de Kaspersky Security Center, establezca la configuración de interfaz en las propiedades de la directiva de Kaspersky Endpoint Security para Windows como se describe a continuación. Al aplicar estos ajustes, evitará el acceso no autorizado a Kaspersky Endpoint Security para Windows en las estaciones de trabajo e impedirá que se realicen cambios en la configuración de esta aplicación.

Para consultar la descripción de estas propiedades de directiva, consulte la Ayuda de Kaspersky Endpoint Security para Windows.

*Para aplicar los ajustes de interfaz recomendados:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en la directiva de Kaspersky Endpoint Security para Windows.

   Se abrirá la ventana de propiedades de la directiva seleccionada.
3. En las propiedades de la directiva, vaya a **Configuración de la aplicación** → **Configuración general** → **Interfaz**.
4. En **Interacción con el usuario**, seleccione la opción **No mostrar interfaz del usuario**. Al seleccionar esta opción, la interfaz de usuario de Kaspersky Endpoint Security para Windows no será visible en las estaciones de trabajo y, en consecuencia, los usuarios no podrán modificar la configuración de Kaspersky Endpoint Security para Windows.
5. En **Protección con contraseña**, habilite el conmutador. Esta opción reduce el riesgo de que la configuración de Kaspersky Endpoint Security para Windows se modifique por error o sin autorización en las estaciones de trabajo.

Se aplican los ajustes recomendados para la interfaz de Kaspersky Endpoint Security para Windows.

## Guardar eventos de directivas importantes en la base de datos del Servidor de administración

Recomendamos guardar únicamente eventos que sean de importancia en la base de datos del Servidor de administración; ello ayudará a no sobrepasar la capacidad de esta base de datos.

*Para que se registren los eventos más importantes en la base de datos del Servidor de administración, haga lo siguiente:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en la directiva de Kaspersky Endpoint Security para Windows.

   Se abrirá la ventana de propiedades de la directiva seleccionada.
3. En las propiedades de la directiva, abra la pestaña **Configuración de eventos**.

4. En la sección **Crítico**, haga clic en **Agregar evento** y active únicamente las casillas de verificación ubicadas junto a los siguientes eventos:

    - *Contrato de licencia de usuario final infringido*
    - *La autoejecución de la aplicación está deshabilitada*
    - *Error de activación*
    - *Se detectó una amenaza activa; ejecute la Desinfección avanzada*
    - *No se puede desinfectar*
    - *Se detectó un vínculo peligroso que ya se había abierto*
    - *Proceso finalizado*
    - *Actividad de red bloqueada*
    - *Ataque de red detectado*
    - *Inicio de aplicación prohibido*
    - *Acceso denegado (bases de datos locales)*
    - *Acceso denegado (KSN)*
    - *Error de actualización local*
    - *No se pueden iniciar dos tareas al mismo tiempo*
    - *Error de interacción con Kaspersky Security Center*
    - *No se actualizaron todos los componentes*
    - *Error al implementar las reglas de cifrado o descifrado de archivos*
    - *Error al habilitar el modo portátil*
    - *Error al deshabilitar el modo portátil*
    - *No se pudo cargar el módulo de cifrado*
    - *No se puede aplicar la directiva*
    - *Error al cambiar los componentes de la aplicación*

5. Haga clic en **Aceptar**.

6. En la sección **Error funcional**, haga clic en **Agregar evento** y seleccione solamente la casilla de verificación junto al evento *Configuración incorrecta de la tarea. Ajustes no aplicados*.

7. Haga clic en **Aceptar**.

8. En la sección **Advertencia**, haga clic en **Agregar evento** y marque las casillas solo junto a los siguientes eventos:

    - *Autoprotección deshabilitada*
    - *Componentes de protección deshabilitados*
    - *Clave de reserva incorrecta*
    - *Se detectó software legítimo que los intrusos pueden usar para dañar su equipo o sus datos personales (bases locales)*
    - *Se detectó software legítimo que los intrusos pueden usar para dañar su equipo o sus datos personales (KSN)*
    - *Objeto eliminado*
    - *Objeto desinfectado*
    - *El usuario optó por no implementar la directiva de cifrado*
    - *El administrador restauró el archivo de la cuarentena del servidor de Kaspersky Anti Targeted Attack Platform*
    - *El administrador colocó el archivo en la cuarentena del servidor de Kaspersky Anti Targeted Attack Platform*
    - *Mensaje de bloqueo del inicio de una aplicación para el administrador*
    - *Mensaje de bloqueo del acceso a un dispositivo para el administrador*
    - *Mensaje de bloqueo del acceso a una página web para el administrador*

9. Haga clic en **Aceptar**.

10. En la sección **Información**, haga clic en **Agregar evento** y marque las casillas de verificación ubicadas solo junto a los siguientes eventos:

    - *Se creó una copia de seguridad del objeto*
    - *Inicio de aplicación prohibido en el modo de prueba*

11. Haga clic en **Aceptar**.

En lo sucesivo, la base de datos del Servidor de administración se usará para guardar eventos que sean de importancia.

# Configuración manual de la tarea de grupo para actualizar Kaspersky Endpoint Security

La opción de programación óptima y recomendada para Kaspersky Endpoint Security es **Al descargar nuevas actualizaciones al repositorio** cuando la casilla de verificación **Utilizar retardo aleatorio automático para el inicio de la tarea** está seleccionada.

# Concesión de acceso sin conexión al dispositivo externo bloqueado por Control de dispositivos

En el componente Control de dispositivos de la directiva de Kaspersky Endpoint Security para Windows, puede administrar el acceso de los usuarios a los dispositivos externos que están instalados en el dispositivo cliente o conectados a este (por ejemplo, discos duros, cámaras o módulos de Wi-Fi). Esto le permite proteger el dispositivo cliente de infecciones cuando se conecten estos dispositivos externos y evitar la pérdida o filtración de datos.

Si necesita otorgar acceso temporal al dispositivo externo bloqueado por Control de dispositivos pero no puede agregar el dispositivo a la lista de dispositivos de confianza, puede otorgarle acceso temporal sin conexión. "Acceso sin conexión" significa que el dispositivo cliente no puede acceder a la red.

Solo puede otorgar acceso sin conexión al dispositivo externo bloqueado por Control de dispositivos si la opción **Permitir solicitudes de acceso temporal** está activada en la configuración de la directiva de Kaspersky Endpoint Security para Windows, en la sección **Configuración de la aplicación → Controles de seguridad → Control de dispositivos**.

Para conceder acceso sin conexión al dispositivo externo bloqueado por Control de dispositivos, se deben cumplir las siguientes etapas:

1. En la ventana de diálogo de Kaspersky Endpoint Security para Windows, el usuario del dispositivo que desea acceder al dispositivo externo bloqueado, genera un archivo de solicitud de acceso y lo envía al administrador de Kaspersky Security Center.

2. Al recibir esta solicitud, el administrador de Kaspersky Security Center crea un archivo de clave de acceso y se lo envía al usuario.

3. En la ventana de diálogo de Kaspersky Endpoint Security para Windows, el usuario del dispositivo activa el archivo de clave de acceso y puede acceder de forma temporal al dispositivo externo.

*Para conceder acceso temporal al dispositivo externo bloqueado por Control de dispositivos, haga lo siguiente:*

1. En el menú principal, vaya a **Activos (dispositivos) → Dispositivos administrados**.

   Se muestra la lista de dispositivos administrados.

2. En la lista, seleccione el dispositivo del usuario que haya solicitado acceso al dispositivo externo bloqueado por Control de dispositivos.

   Solo puede seleccionar un dispositivo.

3. Haga clic en el botón de los tres puntos ( **...** ) ubicado sobre la lista de dispositivos administrados. A continuación, haga clic en el botón **Otorgar acceso al dispositivo en modo sin conexión**.

4. En la ventana que se abrirá, **Configuración de la aplicación**, en la sección **Control de dispositivos**, haga clic en el botón **Examinar**.

5. Seleccione el archivo de solicitud de acceso que le haya enviado el usuario y haga clic en el botón **Abrir**. El archivo debe estar en formato AKEY.

   Se muestran los detalles del dispositivo bloqueado para el que el usuario solicitó acceso.

6. Especifique el valor de la configuración de la **Duración del acceso**.

   Esta configuración define el período durante el cual otorga acceso al usuario al dispositivo bloqueado. El valor predeterminado es el valor que especificó el usuario al crear el archivo de solicitud de acceso.

7. Especifique el período de tiempo durante el cual la clave de acceso puede activarse en el dispositivo.

   Esta configuración define el período durante el cual el usuario puede activar el acceso al dispositivo bloqueado con la clave de acceso provista.

8. Haga clic en el botón **Guardar**.

   Esto abre la ventana estándar **Guardar clave de acceso** de Microsoft Windows.

9. Seleccione la carpeta de destino en la que desea guardar el archivo que contiene la clave de acceso para el dispositivo bloqueado.

10. Haga clic en el botón **Guardar**.

Como resultado, cuando envía al usuario el archivo con la clave de acceso y este la activa en la ventana de diálogo de Kaspersky Endpoint Security para Windows, puede acceder de manera temporal al dispositivo bloqueado durante el período especificado.

# Eliminación de aplicaciones o actualizaciones de software de forma remota

*Para eliminar aplicaciones o actualizaciones de software de forma remota desde dispositivos seleccionados:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.

2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. Para la aplicación Kaspersky Security Center, seleccione el tipo de tarea **Desinstalar aplicación de forma remota**.

4. Escriba un nombre para la tarea que está creando.

   El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).

5. Seleccione los dispositivos a los que se asignará la tarea.

6. Seleccione qué tipo de software desea eliminar y luego seleccione aplicaciones, actualizaciones o parches específicos que desee eliminar:

   - **Desinstalar la aplicación administrada**

     Se muestra una lista de aplicaciones de Kaspersky. Seleccione la aplicación que desee eliminar.

   - **Desinstalar la aplicación incompatible**

     Se muestra una lista de aplicaciones incompatibles con las aplicaciones de seguridad de Kaspersky o Kaspersky Security Center. marque las casillas ubicadas al lado de las aplicaciones que desea eliminar.

   - **Desinstalar la aplicación del Registro de aplicaciones**

De forma predeterminada, los Agentes de red envían información al Servidor de administración sobre las aplicaciones instaladas en los dispositivos administrados. La lista de aplicaciones instaladas se almacena en el registro de aplicaciones.

*Para seleccionar una aplicación del registro de aplicaciones:*

a. Haga clic en el campo **Aplicación para desinstalar** y, luego, seleccione la aplicación que desea eliminar.

Si selecciona Agente de red de Kaspersky Security Center al ejecutar la tarea, el estado *Completada correctamente* indica que se inició el proceso de eliminación. Si se elimina el Agente de red de Kaspersky Security Center, el estado no cambia. Si la tarea falla, el estado cambia a *Error*.

b. Especifique las opciones de desinstalación:

- Modo de desinstalación

Seleccione cómo desea eliminar la aplicación:

- **Definir el comando de desinstalación automáticamente**

  Si la aplicación tiene un comando de desinstalación definido por el proveedor de la aplicación, Kaspersky Security Center usará este comando. Le recomendamos que seleccione esta opción.

- **Especificar el comando de desinstalación**

  Seleccione esta opción si desea especificar su propio comando para la desinstalación de la aplicación.

  Le recomendamos que primero intente eliminar la aplicación utilizando la opción **Definir el comando de desinstalación automáticamente**. Si se produce un error durante la desinstalación mediante el comando definido automáticamente, utilice su propio comando.

  Escriba un comando de instalación en el campo y, luego, especifique la siguiente opción:

  Desinstalar con este comando solo si el comando predeterminado no se detectó automáticamente

  Kaspersky Security Center comprueba si la aplicación seleccionada tiene o no un comando de desinstalación definido por el proveedor de la aplicación. Si se encuentra el comando, Kaspersky Security Center lo usará en lugar del comando especificado en el campo **Comando para desinstalar la aplicación**.

  Le recomendamos que habilite esta opción.

- Reiniciar luego de que la aplicación se desinstale correctamente

Si la aplicación requiere que se reinicie el sistema operativo en el dispositivo administrado después de una desinstalación exitosa, el sistema operativo se reinicia automáticamente.

- **Desinstalar el parche, la actualización de software o la aplicación de terceros que especifique**

  Se muestra una lista de actualizaciones, parches y aplicaciones de terceros. Seleccione el elemento que desee eliminar.

  La lista que se muestra es una lista general de aplicaciones y actualizaciones, y no corresponde a las aplicaciones y actualizaciones instaladas en los dispositivos administrados. Antes de seleccionar un elemento, le recomendamos que se asegure de que la aplicación o actualización esté instalada en los dispositivos definidos en el alcance de la tarea. Puede ver la lista de dispositivos en los que está instalada la aplicación o actualización, a través de la ventana de propiedades.

  *Para ver la lista de dispositivos:*

  a. Haga clic en el nombre de la aplicación o actualización.

     Se abre la ventana de propiedades.

  b. Abra la sección **Dispositivos**.

     También puede ver la lista de aplicaciones instaladas y actualizaciones en la ventana de propiedades del dispositivo.

7. Especifique cómo los dispositivos cliente descargarán la utilidad de desinstalación:

- **Con el Agente de red**

  Los archivos se entregan a los dispositivos cliente mediante el Agente de red instalado en esos dispositivos cliente.

  Si esta opción está deshabilitada, los archivos se entregan mediante las herramientas de Microsoft Windows.

  Recomendamos habilitar esta opción cuando la tarea está asignada a dispositivos en los que se ha instalado el Agente de red.

- **Con los recursos del sistema operativo a través del Servidor de administración**

  Los archivos se transmiten a los dispositivos cliente mediante las herramientas del sistema operativo del Servidor de administración. Puede habilitar esta opción si no hay instalado ningún Agente de red en el dispositivo cliente, pero el dispositivo cliente está en la misma red que el Servidor de administración.

- **Con los recursos del sistema operativo a través de los puntos de distribución**

  Los archivos se transmiten a los dispositivos cliente mediante el uso de herramientas del sistema operativo a través de puntos de distribución. Puede habilitar esta opción si existe al menos un punto de distribución en la red.

  Si se habilita la opción **Con el Agente de red**, los archivos se entregan utilizando las herramientas del sistema operativo solo si las herramientas del Agente de red no están disponibles.

- **N.° máximo de descargas simultáneas**

  El número máximo permitido de dispositivos cliente a los que el Servidor de administración puede transmitir simultáneamente los archivos. Cuanto mayor sea este número, más rápido se desinstalará la aplicación, pero la carga en el Servidor de administración será mayor.

- **N.° máximo de intentos de desinstalación**

Si, al ejecutar la tarea *Desinstalar aplicación de forma remota*, Kaspersky Security Center no puede desinstalar una aplicación en un dispositivo administrado dentro del número de ejecuciones del instalador especificadas por el parámetro, Kaspersky Security Center deja de entregar la utilidad de desinstalación a este dispositivo administrado y ya no inicia el instalador en el dispositivo.

El parámetro **N.° máximo de intentos de desinstalación** permite que guarde los recursos del dispositivo administrado, así como reducir el tráfico (desinstalación, ejecución de archivos MSI y mensajes de error).

Los intentos de inicio de tareas recurrentes pueden indicar un problema en el dispositivo que impide la desinstalación. El administrador debe resolver el problema dentro del número especificado de intentos de desinstalación y, luego, debe reiniciar la tarea (manualmente o según una programación).

Si finalmente no se logra la desinstalación, el problema se considera no resuelto y cualquier inicio de tarea adicional se considera costoso en términos de consumo innecesario de recursos y tráfico.

Cuando se crea la tarea, el contador de intentos se establece en `0`. Cada ejecución del instalador que devuelve un error en el dispositivo incrementa la lectura del contador.

Si se superó el número de intentos especificado en el parámetro y el dispositivo está listo para la desinstalación de la aplicación, puede aumentar el valor del parámetro **N.° máximo de intentos de desinstalación** e iniciar la tarea para desinstalar la aplicación. Alternativamente, puede crear una nueva tarea *Desinstalar aplicación de forma remota*.

- **Verificar el tipo de sistema operativo antes de la descarga**

  Antes de transmitir los archivos a los dispositivos cliente, Kaspersky Security Center verifica si la configuración de la utilidad de Instalación puede aplicarse al sistema operativo del dispositivo cliente. Si la configuración no es corresponde, Kaspersky Security Center no transmite los archivos y no intenta instalar la aplicación. A modo de ejemplo, si necesita instalar una aplicación en los dispositivos de un grupo de administración que contenga dispositivos con sistemas operativos diferentes, puede asignar la tarea de instalación al grupo de administración y habilitar esta opción para que la tarea no afecte a aquellos dispositivos que no tengan el sistema operativo pertinente.

- **Utilizar contraseña de desinstalación**

  Este parámetro se muestra si en el paso anterior seleccionó **Desinstalar aplicación administrada** y luego especificó Kaspersky Security Center Network Agent en el campo **Aplicación a desinstalar**.

  Si previamente estableció la contraseña para la desinstalación remota del Agente de red en Configuración de la directiva del Agente de red, seleccione la casilla de verificación **Usar contraseña de desinstalación** y luego ingrese la contraseña de desinstalación en el campo **Contraseña**. Si no estableció la contraseña para la desinstalación remota del Agente de red, no seleccione la casilla de verificación.

8. Defina las opciones de reinicio del sistema operativo:

- **No reiniciar el dispositivo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

- **Reiniciar el dispositivo**

  Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

  Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**

  Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

  Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

  Si no habilita esta opción, la solicitud se mostrará una sola vez.

- **Reiniciar después de (min)**

  Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

  Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de aplicaciones en sesiones bloqueadas**

Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

Esta opción está deshabilitada de forma predeterminada.

9. Si es necesario, agregue las cuentas que se utilizarán para iniciar la tarea de desinstalación remota:

- **No se necesita una cuenta (el Agente de red está instalado)**

  Si selecciona esta opción, no necesitará especificar la cuenta con la que se ejecutará el instalador de la aplicación. Para ejecutar la tarea, se usará la cuenta con la que se haya iniciado el servicio del Servidor de administración.

  Esta opción no está disponible si el Agente de red no se instaló en los dispositivos cliente.

- **Se necesita una cuenta (no se utiliza el Agente de red)**

  Seleccione esta opción si el Agente de red no está instalado en los dispositivos a los que está asignando la tarea *Desinstalar aplicación de forma remota*. En este caso, puede especificar una cuenta de usuario o un certificado SSH para desinstalar la aplicación.

  - **Cuenta local**. Si se selecciona esta opción, especifique la cuenta bajo la que se ejecutará el instalador de aplicación. Haga clic en el botón **Agregar**, seleccione **Cuenta local** y, a continuación, especifique las credenciales de la cuenta de usuario.

    Puede especificar varias cuentas de usuario si, por ejemplo, ninguna de ellas tiene todos los derechos requeridos en todos los dispositivos a los que asigne esta tarea. En este caso, todas las cuentas añadidas se utilizan para ejecutar la tarea, en orden consecutivo de arriba abajo.

  - **Certificado de SSH**. Si desea desinstalar una aplicación de un dispositivo cliente basado en Linux, puede especificar un certificado SSH en lugar de una cuenta de usuario. Haga clic en el botón **Agregar**, seleccione **Certificado de SSH** y, a continuación, especifique las claves pública y privada del certificado.

    Para generar una clave privada, puede utilizar la utilidad ssh-keygen. Tenga en cuenta que Kaspersky Security Center espera que la clave privada esté en formato PEM, pero, de manera predeterminada, la utilidad ssh-keygen genera claves SSH en formato OPENSSH. Kaspersky Security Center no admite el formato OPENSSH. Para crear una clave privada en el formato PEM admitido, agregue la opción -m PEM en el comando ssh-keygen.

    Por ejemplo:

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "<correo electrónico del usuario>"
    ```

10. Si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.

11. Haga clic en el botón **Finalizar**.

    Se crea la tarea y se la agrega a la lista de tareas.

12. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.

13. En la ventana de propiedades de la tarea, configure los ajustes generales de la tarea.

14. Haga clic en el botón **Guardar**.

15. Ejecute la tarea manualmente o espere a que se inicie a consecuencia de la programación configurada para la tarea.

    Al finalizar la tarea de desinstalación remota, la aplicación seleccionada se eliminará de los dispositivos seleccionados.

### Problemas de desinstalación remota

En ocasiones, la desinstalación remota de aplicaciones de terceros puede finalizar con la siguiente advertencia: "La eliminación remota ha finalizado en este dispositivo con advertencias: la aplicación que se quería eliminar no está instalada". Este problema ocurre cuando la aplicación que se pretende desinstalar ya fue desinstalada o se la instaló solo para un usuario individual. Las aplicaciones instaladas para un usuario individual (también denominadas aplicaciones por usuario) se vuelven invisibles y no se pueden desinstalar de forma remota si el usuario no inició sesión.

Este comportamiento es diferente al de las aplicaciones diseñadas para ser utilizadas por múltiples usuarios en el mismo dispositivo (también denominadas aplicaciones por dispositivo). Las aplicaciones por dispositivo son visibles y accesibles para todos los usuarios del dispositivo.

Por lo tanto, las aplicaciones por usuario deben desinstalarse solo cuando el usuario inicia sesión.

### Orígenes de la información acerca de aplicaciones instaladas

El Agente de red recupera información sobre el software instalado en los dispositivos Windows de las siguientes claves de registro:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

  Contiene información sobre las aplicaciones instaladas para todos los usuarios.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

  Contiene información sobre las aplicaciones instaladas para todos los usuarios.

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

  Contiene información sobre las aplicaciones que el usuario actual tiene instaladas.

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

  Contiene información sobre las aplicaciones instaladas para usuarios específicos.

## Tareas

Esta sección describe tareas utilizadas por Kaspersky Security Center.

# Acerca de las tareas

Kaspersky Security Center administra las aplicaciones de seguridad de Kaspersky instaladas en los dispositivos mediante la creación y ejecución de *tareas*. Las tareas son el medio que se utiliza para instalar, iniciar y detener aplicaciones, analizar archivos, actualizar bases de datos y módulos de software y realizar otras acciones en las aplicaciones.

Si desea utilizar Kaspersky Security Center Web Console para crear una tarea para una aplicación específica, deberá haber instalado el complemento de administración correspondiente a esa aplicación en el Servidor de Kaspersky Security Center Web Console.

Una tarea se puede ejecutar en el Servidor de administración o en un dispositivo.

Las tareas que se realizan en el Servidor de administración incluyen lo siguiente:

- Distribución automática de informes
- Descarga de actualizaciones en el repositorio
- Copia de seguridad de los datos del Servidor de administración
- Mantenimiento de la base de datos

Los siguientes tipos de tareas se ejecutan en los dispositivos:

- *Tareas locales*. Son tareas que se ejecutan en un dispositivo específico.

  Las tareas locales pueden ser modificadas por el administrador usando herramientas de la Consola de administración, o por el usuario de un dispositivo remoto (por ejemplo, a través de la interfaz de aplicaciones de seguridad). Si el administrador y el usuario del dispositivo administrado modifican una tarea local al mismo tiempo, los cambios realizados por el administrador se consideran prioritarios y son los que entran en vigor.

- *Tareas de grupo*. Son tareas que se ejecutan en todos los dispositivos de un grupo específico.

  A menos que se especifique lo contrario en las propiedades de la tarea, una tarea de grupo también afecta a todos los subgrupos del grupo seleccionado. Una tarea de grupo también afecta (opcionalmente) a los dispositivos que se han conectado a Servidores de administración secundarios y virtuales incluidos en el grupo o en cualquiera de sus subgrupos.

- Tareas globales. Son tareas que se ejecutan en un conjunto de dispositivos que pueden o no pertenecer a un grupo.

Para cada aplicación, puede crear cualquier número de tareas de grupo, tareas globales o tareas locales.

Puede copiar, importar, exportar y eliminar tareas, consultar el progreso de su ejecución y modificar su configuración.

Para que una tarea se inicie en un dispositivo, la aplicación para la que se la ha creado debe estar en ejecución.

Los resultados de ejecución de las tareas se guardan en el registro de eventos del sistema operativo en cada dispositivo, en el registro de eventos del sistema operativo en el Servidor de administración y en la base de datos del Servidor de administración.

No incluya datos privados en la configuración de las tareas. Por ejemplo, evite especificar la contraseña del administrador del dominio.

## Acerca del alcance de las tareas

El *alcance de una tarea* es el conjunto de dispositivos en los que se realiza esa tarea. Los tipos de alcance son los siguientes:

- Para una *tarea local*, el alcance es el propio dispositivo.
- Para una *tarea del Servidor de administración*, el alcance es el Servidor de administración.
- Para una *tarea de grupo*, el alcance es la lista de dispositivos incluidos en el grupo.

Al crear una *tarea global*, puede usar los siguientes métodos para especificar su alcance:

- Especificar dispositivos puntuales manualmente.

  Para indicar la dirección de cada dispositivo, puede utilizar una dirección IP (o un intervalo IP), un nombre NetBIOS o un nombre DNS.

- Importar una lista de dispositivos de un archivo .TXT que contenga, en líneas separadas, la dirección de cada dispositivo que se quiera agregar.

  Si importa una lista almacenada en un archivo o crea una lista manualmente y elige identificar los dispositivos por nombre, tenga en cuenta que la lista únicamente podrá incluir dispositivos sobre los que ya haya información en la base de datos del Servidor de administración. Dicha información deberá haberse cargado durante la conexión o el descubrimiento de los dispositivos.

- Especificar una selección de dispositivos.

  El alcance de una tarea cambia con el tiempo, según cambia el conjunto de dispositivos incluidos en la selección. Puede generar una selección de dispositivos basada en los atributos de los dispositivos que quiera incluir (por ejemplo, el software instalado) o en las etiquetas asignadas a esos dispositivos. Una selección de dispositivos es la opción más flexible para especificar el alcance de una tarea.

  Las tareas para selecciones de dispositivos siempre son ejecutadas por el Servidor de administración en forma programada. Estas tareas no se pueden ejecutar en dispositivos que carecen de conexión con el Servidor de administración. Las tareas cuyo alcance se especifica mediante otros métodos se ejecutan directamente en los dispositivos y, por lo tanto, no dependen de la conexión del dispositivo al Servidor de administración.

Las tareas para selecciones de dispositivos no se ejecutan según la hora local del dispositivo, sino según la hora local del Servidor de administración. Cuando el alcance se especifica por otros medios, la tarea se ejecuta según la hora local del dispositivo.

## Crear una tarea

*Para crear una tarea:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga las instrucciones.
3. Si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.
4. Haga clic en el botón **Finalizar**.

Se crea la tarea y se la agrega a la lista de tareas.

*Para crear una nueva tarea asignada a los dispositivos seleccionados:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.

   Se muestra la lista de dispositivos administrados.
2. En la lista de dispositivos administrados, seleccione las casillas de verificación junto a los dispositivos para ejecutar la tarea para ellos. Puede utilizar las funciones de búsqueda y filtrado para encontrar los dispositivos que está buscando.
3. Haga clic en el botón **Ejecutar una tarea** y, luego, seleccione **Agregar una nueva tarea**.

   Se inicia el Asistente para crear nueva tarea.

   En el primer paso del asistente, puede eliminar los dispositivos seleccionados para incluirlos en el alcance de la tarea. Siga las instrucciones del asistente.
4. Haga clic en el botón **Finalizar**.

La tarea se crea para los dispositivos seleccionados.

## Iniciar una tarea manualmente

La aplicación inicia las tareas siguiendo la programación configurada en las propiedades de cada tarea. Puede iniciar una tarea de forma manual en cualquier momento desde la lista de tareas. Como alternativa, puede seleccionar dispositivos en la lista **Dispositivos administrados** y, luego, iniciar una tarea existente para ellos.

*Para iniciar una tarea manualmente:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. En la lista de tareas, marque la casilla ubicada junto a la tarea que desee iniciar.
3. Haga clic en el botón **Iniciar**.

Se inicia la tarea. Puede verificar el estado de la tarea en la columna **Estado** o haciendo clic en el botón **Resultado**.

## Ver la lista de tareas

Puede ver la lista de tareas que se crean en Kaspersky Security Center.

*Para ver la lista de tareas:*

En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.

Se muestra la lista de tareas. Las tareas se agrupan en torno a los nombres de las aplicaciones con las que están relacionadas. Por ejemplo, la tarea *Desinstalar aplicación de forma remota* está relacionada con el Servidor de administración y *Buscar vulnerabilidades y actualizaciones requeridas* se refiere al Agente de red.

*Para ver las propiedades de una tarea:*

Haga clic en el nombre de la tarea.

Aparece la ventana de propiedades de la tarea. En ella encontrará una serie de pestañas con nombre. La pestaña llamada **General** contiene la propiedad **Tipo de tarea**, por ejemplo, y si ingresa a la pestaña **Programación**, encontrará la programación de la tarea.

## Configuración general de tareas

En esta sección, se enumeran los ajustes que puede ver y configurar en la mayoría de las tareas. La lista de ajustes disponibles depende de la tarea que se está configurando.

## Ajustes que se configuran al crear una tarea

A continuación, se enumeran los ajustes que puede definir al momento de crear una tarea. Algunos de estos ajustes también se pueden modificar en las propiedades de la tarea creada.

- Ajustes de reinicio del sistema operativo:
  - **No reiniciar el dispositivo**

    Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

  - **Reiniciar el dispositivo**

    Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

  - **Solicitar al usuario una acción**

    A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

    Esta opción está seleccionada de forma predeterminada.

  - **Repetir solicitud cada (min)**

    Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

    Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

    Si no habilita esta opción, la solicitud se mostrará una sola vez.

  - **Reiniciar después de (min)**

    Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

    Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

  - **Forzar el cierre de aplicaciones en sesiones bloqueadas**

Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

Esta opción está deshabilitada de forma predeterminada.

- Programación de la tarea:

  Los tipos de programación pueden variar según la tarea.

  - **Iniciar tarea (ajuste):**

    - Cada N horas

      La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

      De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

    - Cada N días

      La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

      De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

    - Cada N minutos

      La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

      De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

    - Por días de la semana

      La tarea se ejecutará periódicamente en los días de la semana y a la hora que indique.

      De manera predeterminada, la tarea se ejecutará todos los viernes a las 18:00:00.

    - Mensual

La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

- **Manual**

  La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

  Esta opción está seleccionada de forma predeterminada.

- **Una vez**

  La tarea se ejecuta una vez, en la fecha y hora especificadas (de manera predeterminada, el día en que se creó la tarea).

- **Inmediatamente**

  La tarea se ejecuta inmediatamente después de guardar su configuración.

- **Cada mes en los días especificados de semanas seleccionadas**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  por defecto, la hora de inicio es a las 18:00 y no se selecciona ningún día del mes.

  Tenga en cuenta que no selecciona una fecha específica en el mes, ni el número de la semana (primera, segunda semana del mes), sino el número de secuencia del día de la semana dentro de un mes. Por ejemplo, si coloca el cursor en la celda Mar de la primera fila, significa que la tarea se ejecutará el primer Martes de cada mes nuevo.**MaPrimero**

  Puede seleccionar varios días de la semana.

- **Al descargar nuevas actualizaciones al repositorio**

  La tarea se ejecuta después de descargar las actualizaciones en el repositorio. Por ejemplo, es posible que desee utilizar este programa para la tarea de encontrar vulnerabilidades y actualizaciones necesarias.

- **Ante brotes de virus**

La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

- Antivirus para estaciones de trabajo y servidores de archivos
- Antivirus para defensa del perímetro
- Antivirus para sistemas de correo

Por defecto, están seleccionados todos los tipos de aplicaciones.

En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- Al completarse otra tarea

  La tarea actual se iniciará después de que se complete otra tarea. Esta opción solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

- Ejecutar tareas no realizadas

  Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

  Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

  Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

  Esta opción está deshabilitada de forma predeterminada.

- Utilizar retardo aleatorio automático para el inicio de la tarea

Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

- **Utilizar el retardo aleatorio automático para el inicio de la tarea dentro de un intervalo de**

Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

- Dispositivos a los que se asignará la tarea:
  - **Seleccionar dispositivos de la red detectados por el Servidor de administración**

    La tarea se asignará a ciertos dispositivos específicos. Estos pueden ser tanto dispositivos asignados a grupos de administración como dispositivos no asignados.

    Podría usar esta opción para, por ejemplo, una tarea que instale el Agente de red en los dispositivos que no estén asignados a un grupo de administración.

  - **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**

    Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

    Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.

  - **Asignar tarea a una selección de dispositivos**

    La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

    Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

  - **Asignar tarea a un grupo de administración**

    La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

    Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

    Si se asigna una tarea a un grupo de administración, la pestaña **Seguridad** no se muestra en la ventana de propiedades de la tarea porque las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

- Ajustes de cuenta:
  - **Cuenta predeterminada**

    La tarea se ejecutará utilizando la misma cuenta que la aplicación que realizará la tarea.

    Esta opción está seleccionada de forma predeterminada.

  - **Especificar cuenta**

    Complete los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta con la que se ejecutará la tarea. La cuenta debe tener los derechos necesarios para realizar la tarea.

  - **Cuenta**

Cuenta con la que se ejecutará la tarea.

- **Contraseña**

  Contraseña de la cuenta con la que se ejecutará la tarea.

## Ajustes que se configuran tras crear una tarea

Los siguientes ajustes pueden definirse solamente cuando la tarea ya se ha creado.

- Ajustes para tareas de grupo:
  - **Distribuir a subgrupos**

    Esta opción solo está disponible en los ajustes de tareas de grupo.

    Cuando esta opción está habilitada, el alcance de la tarea incluye lo siguiente:

    - El grupo de administración que se seleccionó al crear la tarea.
    - Los grupos de administración subordinados al grupo de administración seleccionado y ubicados en cualquier nivel de la jerarquía de grupos.

    Cuando esta opción está deshabilitada, el alcance de la tarea incluye solo el grupo de administración que se seleccionó al crear la tarea.

    Esta opción está activada de forma predeterminada.

  - **Distribuir a Servidores de administración secundarios y virtuales**

    Cuando esta opción está habilitada, la tarea aplicada al Servidor de administración principal se aplica también a los servidores de administración secundarios (incluidos los virtuales). Si ya existe una tarea del mismo tipo en un Servidor de administración secundario, se aplican ambas tareas a ese servidor (la existente y la heredada del Servidor de administración principal).

    Esta opción solo está disponible cuando la opción **Distribuir a subgrupos** está habilitada.

    Esta opción está deshabilitada de forma predeterminada.

- Ajustes de programación avanzados:
  - **Encender dispositivos mediante la función Wake-on-LAN antes de iniciar la tarea**

    El sistema operativo del dispositivo se iniciará a la hora especificada antes de que se ejecute la tarea. El período de tiempo predeterminado es de cinco minutos.

    Habilite esta opción si desea que la tarea se ejecute en todos los dispositivos cliente que formen parte del alcance de la tarea, incluidos aquellos que se encuentren apagados cuando la tarea esté próxima a comenzar.

    Si desea que el dispositivo se apague automáticamente una vez completada la tarea, habilite la opción **Apagar dispositivos cuando se complete la tarea**. Encontrará esta opción en la misma ventana.

    Esta opción está deshabilitada de forma predeterminada.

  - **Apagar los dispositivos después de completar la tarea**

    Esta opción puede ser útil para, por ejemplo, una tarea que actualice los dispositivos cliente todos los viernes después del horario laboral y luego los apague para que no consuman energía el fin de semana.

    Esta opción está deshabilitada de forma predeterminada.

- **Detener la tarea si tarda más de**

  Una vez que transcurra el período especificado, la tarea se detendrá automáticamente, se haya completado o no.

  Habilite esta opción si desea que las tareas que tarden mucho en completarse se interrumpan o se detengan.

  Esta opción está deshabilitada de forma predeterminada. El tiempo de ejecución por defecto para las tareas es de 120 minutos.

- Ajustes de notificaciones:
  - Bloque **Almacenar el historial de la tarea**:
    - Guardar en la base de datos del Servidor de administración por (días)

      El Servidor de administración conservará por el número de días especificado los eventos de la aplicación que estén relacionados con la ejecución de la tarea en los dispositivos cliente incluidos en el alcance de la tarea. Transcurrido este período, la información se eliminará del Servidor de administración.

      Esta opción está activada de forma predeterminada.

    - Guardar en el registro de eventos del SO del dispositivo

      Los eventos de la aplicación relacionados con la ejecución de la tarea se almacenarán localmente en el registro de eventos de Windows de cada dispositivo cliente.

      Esta opción está deshabilitada de forma predeterminada.

    - Guardar en el registro de eventos del SO del Servidor de administración

      Los eventos de la aplicación que estén relacionados con la ejecución de la tarea en los dispositivos cliente incluidos en el alcance de la tarea se almacenarán centralmente, en el registro de eventos de Windows del equipo en el que esté instalado el Servidor de administración.

      Esta opción está deshabilitada de forma predeterminada.

    - Guardar todos los eventos

      Si selecciona esta opción, se guardarán todos los sucesos vinculados a la tarea en los registros de eventos.

    - Guardar eventos relacionados con el progreso de la tarea

      Si selecciona esta opción, se guardarán solo aquellos sucesos que estén vinculados con la ejecución de la tarea en los registros de eventos.

    - Guardar solo los resultados de la ejecución de la tarea

      Si selecciona esta opción, se guardarán solo aquellos sucesos que estén vinculados con los resultados de la tarea en los registros de eventos.

  - Notificar los resultados de ejecución de la tarea al administrador

    Puede seleccionar los métodos que se usarán para notificar a los administradores sobre los resultados de la ejecución de la tarea. Los métodos posibles son el correo electrónico, los mensajes SMS y la ejecución de un archivo. Para configurar el mecanismo de notificación, haga clic en el vínculo **Configuración**.

    De forma predeterminada, todos los métodos de notificación están deshabilitados.

- Notificar solo acerca de los errores

  Si esta opción está habilitada, los administradores recibirán una notificación solo si ocurre un error al ejecutar la tarea.

  Si esta opción está deshabilitada, los administradores recibirán una notificación cada vez que se complete la tarea.

  Esta opción está activada de forma predeterminada.

- Los ajustes de seguridad.
- Configuración de la cobertura de la tarea.

  Dependiendo de cómo se determine el alcance de la tarea, estarán presentes los siguientes ajustes:

  - Dispositivos

    Si el alcance de la tarea está determinado por un grupo de administración, verá el nombre del grupo. No podrá hacer ningún cambio. Sin embargo, podrá configurar **Exclusiones del alcance de la tarea**.

    Si el alcance de la tarea está determinado por una lista de dispositivos, podrá agregar y eliminar dispositivos en la lista.

  - Selección de dispositivos

    Podrá cambiar la selección de dispositivos a la que se aplicará la tarea.

  - Exclusiones del alcance de la tarea

    Podrá definir grupos de dispositivos a los que no se aplicará la tarea. Los grupos excluidos solo pueden ser subgrupos del grupo de administración al que se aplica la tarea.

- **Historial de revisiones**.

## Exportar una tarea

Kaspersky Security Center permite guardar una tarea y su configuración en un archivo KLT. El archivo KLT puede usarse para importar la tarea guardada en Kaspersky Security Center Windows o Kaspersky Security Center Linux.

*Para exportar una tarea:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Marque la casilla ubicada junto a la tarea que desee exportar.

   No es posible exportar más de una tarea a la vez. Si selecciona más de una tarea, el botón **Exportar** se desactivará. Las tareas del Servidor de administración tampoco pueden exportarse.

3. Haga clic en el botón **Exportar**.

4. En la ventana **Guardar como** que se abrirá, ingrese la ruta y el nombre del archivo en que se guardará la tarea. Haga clic en el botón **Guardar**.

   La ventana **Guardar como** aparecerá solo si utiliza los navegadores Google Chrome, Microsoft Edge u Opera. Si utiliza otro navegador, el archivo de la tarea se guardará automáticamente en la carpeta **Descargas**.

## Importar una tarea

Kaspersky Security Center permite importar una tarea guardada en un archivo KLT. El archivo KLT contiene la tarea exportada y su configuración.

*Para importar una tarea:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.

2. Haga clic en el botón **Importar**.

3. Haga clic en el botón **Examinar** para elegir el archivo de tareas que desee importar.

4. En la ventana que se abrirá, ingrese la ruta al archivo KLT de la tarea y haga clic en el botón **Abrir**. Tenga en cuenta que no podrá seleccionar más de un archivo de tarea.

   Comenzará a procesarse la tarea.

5. Una vez que la tarea se haya procesado, seleccione los dispositivos a los que desee asignarla. Para ello, seleccione una de las siguientes opciones:

   - **Asignar tarea a un grupo de administración**

     La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

     Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

     Si la tarea se asigna a un grupo de administración, la pestaña **Seguridad** no se mostrará en la ventana de propiedades de la tarea; esto se debe a que las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

   - **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**

     Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

     Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.

   - **Asignar tarea a una selección de dispositivos**

     La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

     Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

6. Elija el alcance de la tarea.

7. Haga clic en el botón **Completado** para finalizar la importación de la tarea.

Aparecerá una notificación con los resultados de la importación. Si la tarea se importa correctamente, puede hacer clic en el vínculo **Detalles** para ver las propiedades de la misma.

Una vez que se complete la importación, la tarea aparecerá en la lista de tareas. También se importarán la configuración y la programación de la tarea. La tarea se iniciará de acuerdo con su programación.

Si la tarea importada tiene el mismo nombre que una tarea existente, el nombre de la tarea importada se complementará con un índice secuencial en formato **(<siguiente número secuencial>)**, por ejemplo **(1)** o **(2)**.

## Iniciar el Asistente para cambiar contraseñas de tareas

Para una tarea no local, puede especificar una cuenta en la que se debe ejecutar la tarea. La cuenta puede definirse al momento de crear la tarea; si la tarea ya existe, puede definirse en sus propiedades. Si la cuenta especificada se usa de acuerdo con las instrucciones de seguridad de la organización, estas instrucciones pueden requerir cambiar la contraseña de la cuenta de vez en cuando. Cuando la contraseña de la cuenta caduca y usted configura una nueva, las tareas no se iniciarán hasta que especifique la nueva contraseña válida en las propiedades de la tarea.

El Asistente para cambiar contraseñas de tareas permite reemplazar automáticamente la contraseña antigua por una nueva en todas las tareas en las que se utiliza la cuenta especificada. También puede cambiar la contraseña manualmente en las propiedades de cada tarea.

*Para iniciar el Asistente para cambiar contraseñas de tareas:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Administrar credenciales de cuentas para tareas de inicio**.

Siga las instrucciones del asistente.

## Paso 1. Especificar credenciales

Especifique las nuevas credenciales. Asegúrese de que el sistema (por ejemplo, Active Directory) las considere válidas. Cuando cambia al siguiente paso del asistente, Kaspersky Security Center verifica si el nombre de cuenta especificado coincide con el nombre de cuenta en las propiedades de cada tarea no local. Si los nombres de las cuentas coinciden, la contraseña en las propiedades de la tarea se reemplazará automáticamente por la nueva.

Para especificar las nuevas credenciales, seleccione una de estas opciones:

- **Utilizar cuenta actual**

  El asistente usará el nombre de la cuenta con la que haya iniciado sesión en Kaspersky Security Center Web Console. Usted deberá escribir la contraseña de dicha cuenta en el campo **Contraseña actual para utilizar en las tareas**.

- **Especificar una cuenta distinta**

  Especifique el nombre de la cuenta con la que se iniciarán las tareas. A continuación, escriba la contraseña de dicha cuenta en el campo **Contraseña actual para utilizar en las tareas**.

Si rellena el campo **Contraseña anterior (opcional, si desea sustituirla por la actual)**, Kaspersky Security Center reemplaza la contraseña solo para aquellas tareas en las que se encuentran tanto el nombre de la cuenta como la contraseña anterior. El reemplazo se realiza automáticamente. En todos los demás casos, debe elegir una acción para realizar el siguiente paso del Asistente.

## Paso 2. Seleccionar una acción para realizar

Si no especificó la contraseña anterior en el primer paso del Asistente o si la contraseña anterior especificada no coincide con las contraseñas en las propiedades de las tareas, debe elegir una acción para las tareas encontradas.

*Para elegir una acción para una tarea:*

1. Busque la tarea para la que necesite elegir una acción y seleccione la casilla a su lado.
2. Realice una de las siguientes acciones:
   - Si desea eliminar la contraseña de las propiedades de la tarea, haga clic en **Eliminar credenciales**.

     La tarea pasará a ejecutarse con la cuenta predeterminada.
   - Si desea reemplazar la contraseña con una nueva, haga clic en **Aplicar el cambio de contraseña incluso si la contraseña anterior no se proporcionó o es incorrecta**.
   - Si desea cancelar el cambio de contraseña, haga clic en **No se seleccionó ninguna acción**.

Las acciones que elija se aplicarán cuando avance al siguiente paso del asistente.

### Paso 3. Ver los resultados

En el último paso del asistente, tendrá la oportunidad de ver los resultados de cada una de las tareas encontradas. Para finalizar el Asistente, haga clic en el botón **Finalizar**.

## Crear la tarea Ejecución remota de scripts

Puede crear una tarea *Ejecución remota de scripts* para ejecutar un paquete de instalación en un dispositivo cliente e instalar una aplicación de forma remota.

Un paquete de instalación contiene un archivo ZIP con un conjunto de scripts diseñados para ejecutarse en los dispositivos cliente y un archivo manifest.json. Encontrará más información para crear este tipo de paquete de instalación en este artículo.

> Esta tarea debe iniciarse solo en dispositivos con el Agente de red para Linux.

*Para iniciar una tarea Ejecución remota de scripts:*

1. Vaya al **Asistente para crear nueva tarea** y seleccione el tipo de tarea **Ejecución remota de scripts**.
2. Ingrese el nombre de la tarea y seleccione los dispositivos a los que se la asignará. Haga clic en el botón **Siguiente**.
3. Seleccione un paquete de instalación que esté basado en un archivo ZIP y contenga un archivo manifest.json para ejecución remota.

   Si no desea volver a ejecutar la tarea en dispositivos en los que ya se haya completado, seleccione la opción **No iniciar esta tarea en los dispositivos en los que ya se completó**.

4. Seleccione una cuenta con la que ejecutar la tarea.

   Si selecciona la cuenta predeterminada, el Agente de red (cuenta root) realizará la tarea.

   > Una vez que se ha iniciado la tarea *Ejecución remota de scripts*, la cuenta asignada no se puede cambiar. Para cambiar la cuenta asignada a la tarea, detenga la tarea a través de sus ajustes y vuelva a crear la tarea con los datos de la cuenta correcta.

5. Si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.

6. Haga clic en el botón **Finalizar**.

   Se crea la tarea *Ejecución remota de scripts* y se la agrega a la lista de tareas.

> Después de recibir datos de la tarea *Ejecución remota de scripts*, el Agente de red limita el acceso a los datos recibidos para todos los usuarios, excepto el administrador y el usuario especificado en la configuración de la tarea.

## Instalar aplicaciones en dispositivos a distancia con la tarea Ejecución remota de scripts

La tarea *Ejecución remota de scripts* puede usarse para instalar una aplicación en un dispositivo cliente remoto mediante la creación de un paquete de instalación personalizado.

Encontrará información sobre cómo preparar un archivo para esta tarea en este artículo.

Si desea crear un paquete de instalación que le permita instalar una aplicación en un dispositivo cliente remoto, asegúrese de que el archivo que vaya a cargar para la tarea contenga los siguientes archivos:

- <nombre del paquete>.deb
- install.sh

  ```
  sudo apt-get install <nombre del paquete>.deb
  ```

- manifest.json

### Esquema JSON para la instalación remota de una aplicación

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "install.sh",
      "args": "<Ingrese los argumentos, si es necesario>",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

### Descripción de las matrices

1. `version`: versión del archivo de manifiesto y de la tarea.

   En este momento, el único valor aceptable es 1.

2. Los elementos de la matriz `actions` determinan la composición y el orden de los scripts que se ejecutan en la tarea.

   El orden de ejecución del script corresponde con el índice (ubicación) de un elemento en la matriz.

3. Para cada elemento de la matriz `actions`, se definen los siguientes elementos.

   a. `type`: tipo de comando ejecutable a partir de los scripts. En este momento, el valor siempre es `execute`.

   b. `path`: ruta al archivo de script en el archivo comprimido.

   c. `args`: argumentos que se pasan al script como parte del comando ejecutable.

   d. `results`: matriz que define las acciones posteriores en función del resultado de la tarea.

      1. `code`: valor que devuelve el script.

      2. `next`: acción que se completará a continuación. Con la acción `continue` se ejecuta el siguiente script (el siguiente elemento de la matriz `actions`); por otro lado, con la acción `break` se detiene la tarea.

   e. `default_next`: acción que se realiza si un script devuelve un valor que no está presente en `results`.

Cuando se inicie la tarea *Ejecución remota de scripts*, el Agente de red cargará el paquete de instalación con la aplicación en el dispositivo cliente. Cuando el dispositivo cliente reciba el paquete de instalación, el Agente de red de dicho dispositivo analizará el archivo manifest.json, definirá el orden de ejecución de los scripts y las acciones que deberá llevar a cabo según los resultados y, finalmente, llevará a cabo la ejecución.

Cuando se complete la tarea *Ejecución remota de scripts*, la aplicación quedará instalada en el dispositivo cliente.

## Configurar notificaciones y supervisar la tarea Ejecución remota de scripts

Puede configurar la supervisión, el comportamiento de guardado de eventos y las notificaciones de la tarea *Ejecución remota de scripts*.

*Para ver el estado de Ejecución remota de scripts:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.

   Se muestra la lista de tareas.

2. Seleccione la tarea y haga clic en **Historial del dispositivo**.

   Se muestra el progreso de la tarea.

*Para configurar el comportamiento de guardado de eventos:*

1. En la lista de tareas, haga clic en la tarea y vaya a la pestaña **Configuración**.
2. En la sección **Notificaciones**, haga clic en el botón **Configuración**.
3. Seleccione una de las siguientes opciones sobre cómo se comportará la aplicación al completarse la tarea:

   - **Guardar todos los eventos**.
   - **Guardar eventos relacionados con el progreso de la tarea**.
   - **Guardar solo los resultados de la ejecución de la tarea**.

     Los eventos se guardan en **Historial del dispositivo** y en **Repositorio de eventos**.

     De forma predeterminada, solo se guardan los resultados de la ejecución de la tarea.

     > Si selecciona **Guardar todos los eventos**, solo se guardarán los resultados de la ejecución de la tarea.

4. Si desea conservar los eventos en la base de datos del Servidor de administración, en el registro de eventos del Servidor de administración o en el dispositivo, active la opción correspondiente.

Obtenga más información sobre cómo configurar las notificaciones en este artículo.

## Preparar un archivo para la tarea Ejecución remota de scripts

A continuación, se enumeran los requisitos con los que debe cumplir un archivo basado en un archivo manifest.json que vaya a usarse para la tarea *Ejecución remota de scripts*:

- Formato de archivo: ZIP.
- Tamaño total: no más de 1 GB.

- La cantidad de archivos y carpetas que contenga es ilimitada.

- El archivo de manifiesto en el que se base el archivo debe respetar el siguiente esquema y debe llamarse manifest.json. El esquema se valida solo durante la ejecución de la tarea en un dispositivo.

  Esquema JSON del archivo de manifiesto y descripción de las matrices

Esquema JSON

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema for execute scripts task",
   "type": "object",
    "properties": {
        "version": {
            "type": "integer",
            "enum": [1]
        },
        "actions":{
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "type": {
                        "type": "string",
                        "enum": ["execute"]
                    },
                    "path": {
                        "type": "string"
                    },
                    "args": {
                        "type": "string"
                    },
                    "results":{
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "code": {
                                    "type": "integer",
                                    "minimum": -255,
                                    "maximum": 255
                                },
                                "next":{
                                    "type": "string",
                                    "enum": ["break", "continue"]
                                }
                            },
                            "required": [
                                "code",
                                "next"
                            ]
                        }
                    },
                    "default_next":{
                        "type": "string",
                        "enum": ["break", "continue"]
                    }
                },
                "required": [
                    "type",
                    "path",
```

```
                    "default_next"
                ]
            }
        }
    },
    "required": [
        "version",
        "actions"
    ]
}
```

Ejemplo de archivo de manifiesto

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

- El archivo debe tener la siguiente estructura:

  `manifest.json`

  `<file1>`

<file2>

<folder1>/<file3>

<folder2>/<folder3>/<file4>

...

<fileX>

manifest.json es el archivo de manifiesto de la tarea.

<file1>, ...., <fileX> es el conjunto de archivos con scripts a ejecutar.

## Crear un paquete de instalación basado en un archivo de manifiesto

*Para crear un paquete de instalación basado en un archivo de manifiesto:*

1. Realice una de las siguientes acciones:

   - En el menú principal, vaya a **Descubrimiento y despliegue** → **Despliegue y asignación** → **Paquetes de instalación**.
   - En el menú principal, vaya a **Operaciones** → **Repositorios** → **Paquetes de instalación**.

   Se muestra una lista de paquetes de instalación disponibles en el Servidor de administración.

2. Haga clic en **Agregar**.

   Se inicia el Asistente de nuevo paquete. Avance por el asistente utilizando el botón **Siguiente**.

3. Seleccione **Crear un paquete de instalación para la tarea Ejecutar scripts de forma remota en función de un archivo ZIP con el archivo manifest.json**.

4. Escriba el nombre del paquete y haga clic en el botón **Examinar**.

   Se abre una ventana estándar de Windows **Abrir** en el navegador para que elija un archivo a fin de crear el paquete de instalación.

5. Elija un archivo de almacenamiento ubicado en los discos disponibles. Encontrará información sobre cómo preparar un archivo para esta tarea en este artículo.

   El archivo comienza a cargarse en el Servidor de administración de Kaspersky Security Center.

   Se inicia el proceso para crear el paquete de instalación.

   El asistente le informará cuando finalice el proceso.

   Si no se crea el paquete de instalación, se muestra el mensaje pertinente.

6. Haga clic en el botón **Finalizar** para cerrar el asistente.

El paquete de instalación que ha creado se descarga en la subcarpeta Paquetes de la carpeta compartida del Servidor de administración. Al concluir la descarga, el paquete de instalación aparecerá en la lista de paquetes de instalación.

En la lista de paquetes de instalación disponibles en el Servidor de administración, puede hacer clic en el vínculo con el nombre de un paquete de instalación personalizado para realizar lo siguiente:

- Ver las siguientes propiedades del paquete de instalación:
  - **Nombre.** Nombre del paquete de instalación personalizado.
  - **Origen.** Nombre del proveedor de la aplicación.
  - **Versión.** Versión de la aplicación.
  - **Creado.** Fecha de creación del paquete de instalación.
  - **Modificado.** Fecha de modificación del paquete de instalación.
  - **Ruta.** Ruta al paquete de instalación personalizado en el Servidor de administración.
- Cambiar el nombre del paquete y los parámetros de la línea de comandos. Esta función solo está disponible para paquetes que no se han creado para aplicaciones de Kaspersky.

# Administración de dispositivos cliente

Kaspersky Security Center le permite administrar dispositivos cliente:

- Vea la configuración y los estados de los dispositivos administrados, incluidos los clústeres y las matrices de servidores.
- Configure sus puntos de distribución.
- Administre las tareas.

Puede usar grupos de administración para combinar dispositivos cliente en un conjunto que se puede administrar como una sola unidad. Un dispositivo cliente puede incluirse en un solo grupo de administración. Los dispositivos se pueden asignar a un grupo automáticamente según las **Condiciones de la regla**:

- Crear reglas de movimiento de dispositivos.
- Copiar reglas de movimiento de dispositivos.
- Condiciones para una regla de movimiento de dispositivos.

Puede usar selecciones de dispositivos para filtrar dispositivos según una condición. También puede etiquetar dispositivos para crear selecciones, para buscar dispositivos y para distribuir dispositivos entre grupos de administración.

# Configuración de un dispositivo administrado

*Para ver la configuración de un dispositivo administrado:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.
   Se muestra la lista de dispositivos administrados.
2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo de su interés.

Se muestra la ventana de propiedades del dispositivo seleccionado.

Las siguientes pestañas se muestran en la parte superior de la ventana de propiedades y representan los principales grupos de ajustes:

- General

Esta pestaña incluye las siguientes secciones:

- La sección **General** muestra información general sobre el dispositivo cliente. La información se basa en los datos recibidos durante la última sincronización del dispositivo cliente con el Servidor de administración.

  - **Nombre**

    En este campo, puede ver y modificar el nombre asignado al dispositivo cliente en el grupo de administración.

  - **Descripción**

    En este campo, puede ingresar una descripción adicional para el dispositivo cliente.

  - **Estado del dispositivo**

    Estado del dispositivo cliente, asignado sobre la base de los criterios definidos por el administrador para el estado de protección antivirus del dispositivo y la actividad del dispositivo en la red.

  - **Nombre completo del grupo**

    Grupo de administración en el que está incluido el dispositivo cliente.

  - **Última actualización de las bases de datos antivirus**

    Fecha en que las bases de datos o las aplicaciones del antivirus se actualizaron por última vez en el dispositivo.

  - **Conectado al Servidor de administración**

    Fecha y hora en que el Agente de red instalado en el dispositivo cliente se conectó al Servidor de administración por última vez.

  - **Visible por última vez**

    Fecha y hora en que el dispositivo se vio en la red por última vez.

  - **Versión del Agente de red**

    Versión del Agente de red instalado.

  - **Creado**

    Fecha de creación del dispositivo en Kaspersky Security Center.

- **Propietario del dispositivo**

  Nombre del propietario del dispositivo. Puede asignar o quitar un usuario como propietario del dispositivo haciendo clic en el vínculo **Administrar propietario del dispositivo**.

- **No desconectar del Servidor de administración**

  Si esta opción está habilitada, se mantendrá una conexión continua entre el dispositivo administrado y el Servidor de administración. Esta opción podría resultarle útil si no usa servidores push, que proporcionan este tipo de conectividad.

  Si no habilita esta opción y no utiliza servidores push, el dispositivo administrado se conectará al Servidor de administración únicamente para sincronizar o transmitir información.

  El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

  Esta opción está deshabilitada de manera predeterminada en los dispositivos administrados. Esta opción está habilitada de manera predeterminada en el dispositivo en el que se ha instalado el Servidor de administración y no se puede deshabilitar en ese caso.

- La sección de **Red** muestra la siguiente información sobre las propiedades de red del dispositivo cliente:

  - **Dirección IP**

    Dirección IP del dispositivo.

  - **Dominio de Windows**

    Dominio o grupo de trabajo de Windows en el que está incluido el dispositivo.

  - **Nombre DNS**

    Nombre del dominio DNS del dispositivo cliente.

  - **Nombre NetBIOS**

    Nombre de la red de Windows del dispositivo cliente.

  - **Dirección IPv6**

- La sección **Sistema** proporciona información sobre el sistema operativo instalado en el dispositivo cliente:

  - **Sistema operativo**
  - **Arquitectura de la CPU**
  - **Nombre del dispositivo**
  - **Tipo de máquina virtual**

Fabricante de la máquina virtual.

- **Máquina virtual dinámica como parte de VDI**

  Esta fila muestra si el dispositivo cliente es una máquina virtual dinámica como parte de VDI.

- La sección **Protección** proporciona información sobre el estado actual de la protección antivirus del dispositivo cliente:

  - **Visible**

    Estado de visibilidad del dispositivo cliente.

  - **Estado del dispositivo**

    Estado del dispositivo cliente, asignado sobre la base de los criterios definidos por el administrador para el estado de protección antivirus del dispositivo y la actividad del dispositivo en la red.

  - **Descripción del estado**

    Estado de la protección del dispositivo cliente y de la conexión con el Servidor de administración.

  - **Estado de protección**

    Este campo muestra el estado de la protección en tiempo real registrado en el dispositivo cliente.

    Si el estado se modifica en el dispositivo, el cambio no se verá reflejado en la ventana de propiedades del dispositivo sino hasta que el dispositivo se sincronice con el Servidor de administración.

  - **Último análisis completo**

    Fecha y hora del último análisis antimalware realizado en el dispositivo cliente.

  - **Virus detectados**

    Cantidad total de amenazas detectadas en el dispositivo cliente desde la instalación de la aplicación de seguridad (primer análisis) o desde la última vez que el contador de amenazas se puso en cero.

  - **Objetos que no se pudieron desinfectar**

    Número de archivos no procesados en el dispositivo cliente.

    Este campo no refleja el número de archivos no procesados en dispositivos móviles.

- Estado de cifrado del disco

  Estado del cifrado de archivos en las unidades locales del dispositivo. Para obtener una descripción de los estados, consulte la Ayuda de Kaspersky Endpoint Security para Windows.

- La sección **Estado del dispositivo definido por la aplicación** proporciona información sobre el estado del dispositivo definido por la aplicación administrada instalada en el dispositivo. El estado de este dispositivo puede diferir del definido por Kaspersky Security Center.

- Aplicaciones

  Esta pestaña enumera todas las aplicaciones de Kaspersky instaladas en el dispositivo cliente. Contiene los botones **Iniciar** y **Detener** que le permiten iniciar y detener la aplicación de Kaspersky seleccionada (pero no el Agente de red). Puede usar estos botones si el puerto 15000 UDP está disponible en el dispositivo administrado para recibir notificaciones push del Servidor de administración. Si el dispositivo administrado no está disponible para notificaciones push, pero el modo de conexión continua al Servidor de administración está activado (la opción **No desconectar del Servidor de administración** en la sección **General** está activada), los botones **Iniciar** y **Detener** también están disponibles. De lo contrario, cuando intenta iniciar o detener la aplicación, se muestra un mensaje de error. También puede hacer clic en el nombre de una aplicación para ver información general sobre la aplicación, los ajustes de configuración de la misma y una lista de los eventos ocurridos en el dispositivo.

- Directivas y perfiles de directivas activos

  Esta pestaña enumera las directivas y los perfiles de directivas que están asignados al dispositivo administrado en un momento dado.

- Tareas

  La pestaña **Tareas** permite administrar las tareas del dispositivo cliente. Utilice esta sección para crear tareas nuevas, ver la lista de tareas existentes, ver los resultados de ejecución de las tareas e iniciar, detener, eliminar y reconfigurar las tareas existentes. La lista de tareas mostrada se basa en los datos recibidos durante la última sesión de sincronización entre el cliente y el Servidor de administración. El Servidor de administración solicita detalles sobre el estado de las tareas al dispositivo cliente. Si el puerto 15000 UDP está disponible en el dispositivo administrado para recibir notificaciones push del Servidor de administración, se muestra el estado de la tarea y se activan los botones para administrar la tarea. Si el dispositivo administrado no está disponible para notificaciones push, pero el modo de conexión continua al Servidor de administración está activado (la opción **No desconectar del Servidor de administración** en la sección **General** está activada), las acciones con tareas también están disponibles.

  Si no se establece una conexión, no se muestra el estado y los botones quedan desactivados.

- Eventos

  La pestaña **Eventos** muestra los eventos registrados en el Servidor de administración para el dispositivo cliente seleccionado.

- Problemas de seguridad

  En la pestaña **Problemas de seguridad**, puede ver, crear y editar problemas de seguridad para el dispositivo cliente. Los problemas de seguridad se pueden crear manualmente por el administrador o automáticamente por las aplicaciones de Kaspersky administradas que se han instalado en el dispositivo cliente. El administrador podría crear un problema de seguridad si, por ejemplo, algunos de sus usuarios han copiado malware de una unidad extraíble en más de una ocasión. En el texto del problema de seguridad, el administrador podría brindar una breve descripción del caso, delinear las acciones que recomienda tomar (por ejemplo, medidas disciplinarias contra los usuarios) y agregar un vínculo al usuario o a los usuarios.

  Se denomina *procesado* al problema de seguridad para el cual se han tomado todas las medidas necesarias. La presencia de problemas de seguridad no procesados puede usarse como condición para cambiar el estado de un dispositivo a *Crítico* o *Advertencia*.

  En esta sección, encontrará una lista con problemas de seguridad que se hayan creado para el dispositivo. Los problemas de seguridad se clasifican por tipo y por nivel de gravedad. El tipo de problema de seguridad lo define la aplicación de Kaspersky que crea el problema de seguridad. Si desea resaltar los problemas de seguridad procesados de la lista, marque la casilla de la columna **Procesado**.

- Etiquetas

  La pestaña **Etiquetas** permite administrar la lista de palabras clave que se utilizan para buscar dispositivos cliente. Aquí puede ver la lista de etiquetas existentes, asignar etiquetas incluidas en la lista, configurar reglas de etiquetado automático, agregar etiquetas nuevas, eliminar etiquetas antiguas y modificar el nombre de las etiquetas existentes.

- Avanzado

Esta pestaña incluye las siguientes secciones:

- **Registro de aplicaciones**. En esta sección, puede ver un registro de las aplicaciones instaladas en el dispositivo cliente y de las actualizaciones de esas aplicaciones; también puede configurar el modo de visualización del registro de aplicaciones.

  Podrá ver información sobre las aplicaciones instaladas si el Agente de red instalado en el dispositivo cliente le envía la información necesaria al Servidor de administración. Puede configurar el envío de información al Servidor de administración en la ventana de propiedades del Agente de red o en su directiva, en la sección **Repositorios**.

  Al hacer clic en el nombre de una aplicación, se abre una ventana que contiene los detalles de la aplicación y una lista de los paquetes de actualización instalados para la aplicación.

- **Archivos ejecutables**. Esta sección muestra los archivos ejecutables almacenados en el dispositivo cliente.

- **Puntos de distribución**. Esta sección contiene una lista de los puntos de distribución con los que interactúa el dispositivo.

  - Exportar a archivo

    Haga clic en el botón **Exportar a archivo** para guardar en un archivo la lista de puntos de distribución con los que interactúa el dispositivo. De manera predeterminada, la aplicación exporta la lista de dispositivos a un archivo CSV.

  - Propiedades

    Haga clic en el botón **Propiedades** para ver y configurar el punto de distribución con el que interactúa el dispositivo.

- **Registro de hardware**. En esta sección, puede ver información sobre el hardware instalado en el dispositivo cliente.

  Si el Agente de red está instalado en un dispositivo con Windows, envía al Servidor de administración la siguiente información sobre el hardware del dispositivo:

  - RAM
  - Dispositivos de almacenamiento
  - Placa madre
  - CPU
  - Adaptadores de red
  - Monitores
  - Adaptador de video
  - Tarjeta de sonido

  Si el Agente de red está instalado en un dispositivo con Linux o macOS, envía al Servidor de administración la siguiente información sobre el hardware del dispositivo, si el sistema operativo la proporciona:

- Volumen total de la RAM
- Volumen total de los dispositivos de almacenamiento masivo
- Placa madre
- CPU
- Adaptadores de red

- **Actualizaciones disponibles**. Esta sección muestra las actualizaciones de software que se han encontrado en el dispositivo, pero que aún no se han instalado.

- **Vulnerabilidades de software**. Esta sección muestra información sobre las vulnerabilidades de las aplicaciones de terceros instaladas en los dispositivos cliente.

  Para guardar las vulnerabilidades en un archivo, marque las casillas ubicadas junto a las vulnerabilidades que desea guardar, y luego haga clic en el botón **Exportar a CSV** o en el botón **Exportar a TXT**.

  La sección contiene los siguientes ajustes:

  - Mostrar solo las vulnerabilidades que pueden repararse

    Si habilita esta opción, la sección mostrará las vulnerabilidades que se puedan reparar con un parche.

    Si deshabilita esta opción, la sección mostrará tanto las vulnerabilidades que se puedan reparar con un parche como las vulnerabilidades para las que no exista parche publicado.

    Esta opción está activada de forma predeterminada.

  - Prop. de la vulnerabilidad

    Haga clic en el nombre de una vulnerabilidad de software de la lista para ver las propiedades de la vulnerabilidad de software seleccionada en una ventana aparte. En la ventana, puede hacer lo siguiente:

    - Ignorar la vulnerabilidad de software en el dispositivo administrado (en la Consola de administración o en Kaspersky Security Center Web Console).
    - Ver la lista de reparaciones recomendadas para la vulnerabilidad.
    - Elegir manualmente las actualizaciones de software que se usarán para corregir la vulnerabilidad (en la Consola de administración o en Kaspersky Security Center Web Console).
    - Ver las instancias de la vulnerabilidad.
    - Ver la lista de tareas existentes que permiten reparar la vulnerabilidad y crear tareas de reparación nuevas.

- **Diagnóstico remoto**. En esta sección, puede realizar un diagnóstico remoto de dispositivos cliente.

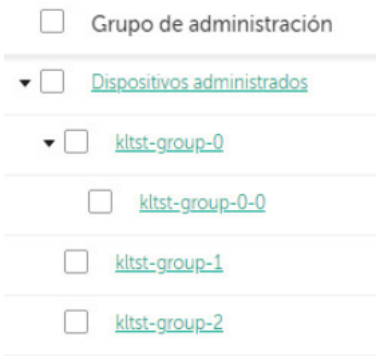
Si usa un DBMS PostgreSQL, MariaDB o MySQL, la pestaña **Eventos** puede mostrar una lista incompleta de eventos para el dispositivo cliente seleccionado. Esto ocurre cuando el DBMS almacena una gran cantidad de eventos. Realice una de las siguientes acciones si desea aumentar la cantidad de eventos mostrados:

- Eliminación de eventos innecesarios.
- Reducción del plazo de almacenamiento para eventos innecesarios.

Para ver una lista completa de eventos registrados en el Servidor de administración para el dispositivo, use Informes.

## Creación de grupos de administración

Inmediatamente después de la instalación de Kaspersky Security Center, la jerarquía de grupos de administración contiene solo un grupo de administración llamado **Dispositivos administrados**. Al crear una jerarquía de grupos de administración, puede añadir dispositivos, incluidas máquinas virtuales, al grupo **Dispositivos administrados** y agregar grupos anidados (consulte la figura a continuación).




Ver jerarquía de grupos de administración

*Para crear un grupo de administración:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Jerarquía de grupos**.
2. En la estructura del grupo de administración, seleccione el grupo de administración donde desea incluir el nuevo grupo de administración.
3. Haga clic en el botón **Agregar**.
4. En la ventana **Nombre del nuevo grupo de administración** que se abre, introduzca el nombre del grupo y haga clic en el botón **Agregar**.

En la jerarquía de grupos de administración, aparecerá un nuevo grupo con el nombre especificado.

La aplicación permite crear una jerarquía de grupos de administración basada en la estructura de Active Directory o en la estructura de la red del dominio. También es posible crear una estructura de grupos a partir de un archivo de texto.

*Para crear una estructura de grupos de administración:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Jerarquía de grupos**.
2. Haga clic en el botón **Importar**.

Se inicia el Asistente de nueva estructura de grupos de administración. Siga las instrucciones del asistente.

## Agregar dispositivos a un grupo de administración en forma manual

Puede mover sus dispositivos a grupos de administración de distintas maneras: puede crear reglas que los muevan automáticamente, puede moverlos de un grupo de administración a otro en forma manual, o puede agregarlos manualmente a un grupo de administración puntual. En esta sección, se explica cómo agregar dispositivos a un grupo de administración de manera manual.

*Para agregar uno o más dispositivos manualmente a un grupo de administración específico:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.
2. Haga clic en el vínculo **Ruta actual:** `<ruta actual>` que se encuentra sobre la lista.
3. En la ventana que se abre, seleccione el grupo de administración al que desee agregar los dispositivos.
4. Haga clic en el botón **Agregar dispositivos**.
   Se inicia el Asistente para mover dispositivos.
5. Cree una lista con los dispositivos que desee agregar al grupo de administración.

   > La base de datos del Servidor de administración debe tener información sobre los dispositivos que quiera agregar. No puede agregar dispositivos que nunca se hayan conectado o que la aplicación aún no haya detectado.

   Elija un método para agregar los dispositivos a la lista:

   - Haga clic en el botón **Agregar dispositivos** y luego elija los dispositivos de una de las siguientes maneras:
     - Seleccione los dispositivos de la lista de dispositivos detectados por el Servidor de administración.
     - Especifique las direcciones IP de los dispositivos o un intervalo de direcciones IP.

       > El rango de direcciones IP no debe contener más de 1 048 576 direcciones.

     - Especifique los nombres NetBIOS o los nombres DNS de los dispositivos.

       > El campo del nombre del dispositivo no debe contener espacios en blanco ni los siguientes caracteres prohibidos: ¡\ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %
   - Haga clic en el botón **Importar dispositivos desde archivo** para importar una lista de dispositivos desde un archivo .txt. Utilice una línea diferente para la dirección o el nombre de cada dispositivo.

     > El archivo no debe contener espacios en blanco ni los siguientes caracteres prohibidos: ¡\ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %

6. Revise la lista de dispositivos que se agregarán al grupo de administración. Si necesita agregar o quitar dispositivos, haga los cambios necesarios en la lista.

7. Si no ve ningún error en la lista, haga clic en el botón **Siguiente**.

El asistente procesará la lista de dispositivos y mostrará el resultado. Los dispositivos que se procesen correctamente se agregarán al grupo de administración y aparecerán en la lista de dispositivos con nombres generados por el Servidor de administración.

## Mover dispositivos o clústeres a un grupo de administración en forma manual

Puede mover dispositivos de un grupo de administración a otro, o del grupo de dispositivos no asignados a un grupo de administración.

También puede mover clústeres o conjuntos de servidores de un grupo de administración a otro. Cuando mueve un clúster o un conjunto de servidores a otro grupo, todos sus nodos se mueven con él, porque un clúster y cualquiera de sus nodos siempre pertenecen al mismo grupo de administración. Cuando selecciona un solo nodo de clúster en la pestaña **Dispositivos**, el botón **Mover a un grupo** deja de estar disponible.

*Para mover uno o varios dispositivos o clústeres a un grupo de administración seleccionado:*

1. Abra el grupo de administración al que pertenezcan los dispositivos que desee mover. Para ello, realice una de las siguientes acciones:

   - Para abrir un grupo de administración, en el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**, haga clic en el vínculo de la ruta en el campo **Ruta actual** y seleccione un grupo de administración en el panel izquierdo que se abre.

   - Para abrir el grupo **Dispositivos no asignados**, en el menú principal, vaya a **Descubrimiento y despliegue** → **Dispositivos no asignados**.

2. Si el grupo de administración contiene clústeres o conjuntos de servidores, la sección **Dispositivos administrados** se divide en dos pestañas: **Dispositivos** y **Clústeres y conjuntos de servidores** Abra la pestaña del objeto que desea mover.

3. Active las casillas ubicadas junto a los dispositivos o clústeres que desee mover a otro grupo.

4. Haga clic en el botón **Mover a un grupo**.

5. En la jerarquía de grupos de administración, marque la casilla ubicada junto al grupo de administración al que desee mover los dispositivos o clústeres seleccionados.

6. Haga clic en el botón **Mover**.

Los dispositivos o clústeres seleccionados se moverán al grupo de administración seleccionado.

## Crear reglas de movimiento de dispositivos

Puede configurar reglas de movimiento de dispositivos; es decir, reglas que asignan automáticamente dispositivos a grupos de administración.

*Para crear una regla de movimiento:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Reglas de movimiento**.
2. Haga clic en **Agregar**.
3. En la ventana que se abre, especifique la siguiente información en la pestaña **General**:

- Nombre de la regla

  Ingrese un nombre para la nueva regla.

  Cuando se copia una regla, la regla nueva recibe el nombre de la regla de origen, con el agregado de un índice numérico entre paréntesis, como (1).

- Grupo de administración

  Seleccione el grupo de administración al que se moverán automáticamente los dispositivos.

- Regla activa

  Si esta opción está habilitada, la regla se habilitará y empezará a operar en cuanto la guarde.

  Si esta opción está deshabilitada, la regla se creará, pero no se activará. No entrará en funcionamiento hasta que habilite esta opción.

- Mover solo los dispositivos que no pertenezcan a un grupo de administración

  Si esta opción está habilitada, solo los dispositivos no asignados se moverán al grupo seleccionado.

  Si esta opción está deshabilitada, tanto los dispositivos no asignados como los dispositivos que ya pertenezcan a otro grupo de administración se moverán al grupo seleccionado.

- Aplicar regla

  Puede seleccionar una de las siguientes opciones:

  - **Ejecutar una vez por dispositivo**

    La regla se aplicará una vez por cada dispositivo que reúna los criterios especificados.

  - **Ejecutar una vez por dispositivo y luego cada vez que se reinstale el Agente de red**

    La regla se aplicará una vez por cada dispositivo que reúna los criterios especificados; tras esa primera aplicación, la regla se aplicará solo cuando el Agente de red se reinstale en esos dispositivos.

  - **Aplicar esta regla continuamente**

    La regla se aplicará siguiendo una programación definida automáticamente por el Servidor de administración (generalmente, una vez cada varias horas).

4. En la pestaña **Condiciones de la regla**, especifique al menos un criterio por el cual los dispositivos se mueven a un grupo de administración.

5. Haga clic en **Guardar**.

Se crea la regla de movimiento. La nueva regla aparece en la lista de reglas de movimiento.

Cuanto más alta sea la posición en la lista, mayor será la prioridad de la regla. Para aumentar o reducir la prioridad de una regla de movimiento, mueva la regla en la lista hacia arriba o hacia abajo, respectivamente, con el mouse.

Si se selecciona la opción **Aplicar esta regla continuamente**, la regla de movimiento se aplica independientemente de la configuración de prioridad. Esas reglas se aplican de acuerdo con la programación que el Servidor de administración configura automáticamente.

Si los atributos de dispositivo cumplen con las condiciones de varias reglas, el dispositivo se mueve al grupo de destino de la regla con la prioridad más alta (es decir, la que tiene la clasificación más alta en la lista de reglas).

## Copiar reglas de movimiento de dispositivos

Puede copiar sus reglas de movimiento de dispositivos si, por ejemplo, desea tener varias reglas de movimiento idénticas para diferentes grupos de administración de destino.

Para copiar una regla de movimiento existente:

1. Realice una de las siguientes acciones:

   - En el menú principal, vaya a **Activos (dispositivos)** → **Reglas de movimiento**.
   - En el menú principal, vaya a **Descubrimiento y despliegue** → **Despliegue y asignación** → **Reglas de movimiento**.

   Se muestra la lista de reglas de movimiento.

2. Marque la casilla ubicada junto a la regla que desee copiar.

3. Haga clic en **Copiar**.

4. En la ventana que se abre, cambie la siguiente información en la pestaña **General** (si desea copiar la regla sin modificar su configuración, no haga ningún cambio):

   - Nombre de la regla

     Ingrese un nombre para la nueva regla.

     Cuando se copia una regla, la regla nueva recibe el nombre de la regla de origen, con el agregado de un índice numérico entre paréntesis, como (1).

   - Grupo de administración

     Seleccione el grupo de administración al que se moverán automáticamente los dispositivos.

   - Regla activa

     Si esta opción está habilitada, la regla se habilitará y empezará a operar en cuanto la guarde.

     Si esta opción está deshabilitada, la regla se creará, pero no se activará. No entrará en funcionamiento hasta que habilite esta opción.

   - Mover solo los dispositivos que no pertenezcan a un grupo de administración

     Si esta opción está habilitada, solo los dispositivos no asignados se moverán al grupo seleccionado.

     Si esta opción está deshabilitada, tanto los dispositivos no asignados como los dispositivos que ya pertenezcan a otro grupo de administración se moverán al grupo seleccionado.

   - Aplicar regla

     Puede seleccionar una de las siguientes opciones:

     - **Ejecutar una vez por dispositivo**

       La regla se aplicará una vez por cada dispositivo que reúna los criterios especificados.

     - **Ejecutar una vez por dispositivo y luego cada vez que se reinstale el Agente de red**

       La regla se aplicará una vez por cada dispositivo que reúna los criterios especificados; tras esa primera aplicación, la regla se aplicará solo cuando el Agente de red se reinstale en esos dispositivos.

     - **Aplicar esta regla continuamente**

       La regla se aplicará siguiendo una programación definida automáticamente por el Servidor de administración (generalmente, una vez cada varias horas).

5. En la pestaña **Condiciones de la regla**, especifique al menos un criterio para los dispositivos que desea que se muevan automáticamente.

6. Haga clic en **Guardar**.

Se crea la nueva regla de movimiento. La nueva regla aparece en la lista de reglas de movimiento.

# Condiciones para una regla de movimiento de dispositivos

Cuando usted crea o copia una regla para mover dispositivos cliente a grupos de administración, establece en la pestaña **Condiciones de la regla** las condiciones mover los dispositivos. Para determinar qué dispositivos mover, puede utilizar los siguientes criterios:

- Etiquetas asignadas a los dispositivos cliente.
- Parámetros de red. Por ejemplo, puede mover dispositivos con direcciones IP de un rango específico.
- Aplicaciones administradas instaladas en dispositivos cliente, por ejemplo, Agente de red o Servidor de administración.
- Máquinas virtuales, que son los dispositivos cliente.
- Información sobre la unidad organizativa (OU) de Active Directory con los dispositivos cliente.
- Información sobre un segmento de nube con los dispositivos cliente.

A continuación, puede encontrar la descripción sobre cómo especificar esta información en una regla de movimiento de dispositivos.

Si especifica varias condiciones en la regla, se usa el operador lógico AND y todas las condiciones se aplican al mismo tiempo. Si no selecciona ninguna opción o deja algunos campos en blanco, dichas condiciones no se aplican.

## Pestaña Etiquetas

En esta pestaña, puede configurar una búsqueda del dispositivo según las etiquetas para dispositivos que se añadieron anteriormente a las descripciones de los dispositivos administrados: Para hacerlo, seleccione las etiquetas pertinentes. Además, puede habilitar las siguientes opciones:

- **Aplicar a los dispositivos que no tengan las etiquetas especificadas**

  Si esta opción está habilitada, todos los dispositivos con las etiquetas especificadas se excluyen de una regla de movimiento de dispositivos. Si esta opción está deshabilitada, la regla de movimiento de dispositivos se aplica a los dispositivos con todas las etiquetas seleccionadas.

  Esta opción está deshabilitada de forma predeterminada.

- **Aplicar si coincide al menos una etiqueta especificada**

  Si esta opción está habilitada, se aplica una regla de movimiento de dispositivos a los dispositivos cliente con al menos una de las etiquetas seleccionadas. Si esta opción está deshabilitada, la regla de movimiento de dispositivos se aplica a los dispositivos con todas las etiquetas seleccionadas.

  Esta opción está deshabilitada de forma predeterminada.

## Pestaña Red

En esta pestaña, puede especificar los datos de red de los dispositivos a los que atañe una regla de movimiento de dispositivos:

- **Nombre del dispositivo en la red de Windows**

  Nombre de red de Windows (nombre NetBIOS) del dispositivo, o la dirección IPv4 o IPv6.

- **Dominio de Windows**

  Una regla de movimiento de dispositivos se aplica a todos los dispositivos incluidos en el dominio de Windows especificado.

- **Nombre DNS del dispositivo**

  Nombre de dominio DNS del dispositivo cliente que desea mover. Complete este campo si su red incluye un servidor DNS.

  Si la intercalación con diferenciación entre mayúsculas y minúsculas está configurada para la base de datos utilizada para Kaspersky Security Center, respete las mayúsculas y minúsculas cuando ingrese el nombre DNS de un dispositivo. De lo contrario, la regla de movimiento de dispositivos no funcionará.

- **Dominio DNS**

  Una regla de movimiento de dispositivos se aplica a todos los dispositivos incluidos en el sufijo DNS principal especificado. Complete este campo si su red incluye un servidor DNS.

- **Intervalo IP**

  Si habilita esta opción, podrá ingresar las direcciones IP inicial y final del intervalo IP en el que deberán estar incluidos los dispositivos pertinentes.

  Esta opción está deshabilitada de forma predeterminada.

- **Dirección IP para establecer conexión con el Servidor de administración**

  Si esta opción está habilitada, puede configurar las direcciones IP mediante las cuales los dispositivos cliente se conectan al Servidor de administración. Para hacerlo, especifique el rango de IP que incluye todas las direcciones IP necesarias.

  Esta opción está deshabilitada de forma predeterminada.

- **El dispositivo se encuentra en este intervalo IP**

  Si esta opción está activada, puede seleccionar un rango de IP que haya agregado previamente en la sección **Intervalos IP**. Los dispositivos relevantes deben estar incluidos en el rango IP seleccionado.

  Esta opción está deshabilitada de forma predeterminada.

- Perfil de conexión cambiado

  Seleccione uno de los siguientes valores:

  - **Sí**. Una regla de movimiento de dispositivos solo se aplica a los dispositivos cliente con un perfil de conexión modificado.
  - **No**. La regla de movimiento de dispositivos solo se aplica a los dispositivos cliente cuyo perfil de conexión no cambió.
  - **Ningún valor seleccionado**. La condición no se aplica.

- Administrado por un Servidor de administración diferente

  Seleccione uno de los siguientes valores:

  - **Sí**. Una regla de movimiento de dispositivos solo se aplica a los dispositivos cliente administrados por otros Servidores de administración. Estos servidores son diferentes del servidor en el que configura la regla de movimiento de dispositivos.
  - **No**. La regla de movimiento de dispositivos solo se aplica a los dispositivos cliente administrados por el Servidor de administración actual.
  - **Ningún valor seleccionado**. La condición no se aplica.

## Pestaña Aplicaciones

En esta pestaña, puede configurar una regla de movimiento de dispositivos basada en las aplicaciones administradas y los sistemas operativos instalados en los dispositivos cliente:

- Agente de red instalado

  Seleccione uno de los siguientes valores:

  - **Sí**. Una regla de movimiento de dispositivos solo se aplica a los dispositivos cliente con el Agente de red instalado.
  - **No**. La regla de movimiento de dispositivos solo se aplica a los dispositivos cliente en los que el Agente de red no está instalado.
  - **Ningún valor seleccionado**. La condición no se aplica.

- Aplicaciones

  Especifique qué aplicaciones administradas deben instalarse en los dispositivos cliente, de modo que se aplique una regla de movimiento de dispositivos a estos dispositivos. Por ejemplo, puede seleccionar **Agente de red de Kaspersky Security Center 15.1** o **Servidor de administración de Kaspersky Security Center 15.1**.

  Si no selecciona ninguna aplicación administrada, la condición no se aplica.

- Versión del sistema operativo

  Puede seleccionar dispositivos cliente en función de la versión del sistema operativo. Para ello, especifique los sistemas operativos que deben instalarse en los dispositivos cliente. Como resultado, se aplica una regla de movimiento de dispositivos a los dispositivos cliente con los sistemas operativos seleccionados.

  Si no habilita esta opción, la condición no se aplica. La opción está desactivada de forma predeterminada.

- Arquitectura del sistema operativo

  Puede seleccionar dispositivos cliente según el tamaño de bits del sistema operativo. En el bloque **Arquitectura del sistema operativo**, puede seleccionar uno de los siguientes valores:

  - **Desconocido**
  - **x86**
  - **AMD64**
  - **IA64**

  *Para comprobar el tamaño de bits del sistema operativo de los dispositivos cliente:*

  1. En el menú principal, vaya a la sección **Activos (dispositivos)** → **Dispositivos administrados**.
  2. Haga clic en el botón **Configuración de las columnas** ( ⚙ ) a la derecha.
  3. Seleccione la opción **Arquitectura del sistema operativo**, y haga clic en el botón **Guardar**.

     Después, se muestra el tamaño de bits del sistema operativo para cada dispositivo administrado.

- Versión del Service Pack del sistema operativo

  En este campo, puede especificar la versión del paquete de su sistema operativo (en formato *X.Y*), que determinará cómo aplicar la regla de migración a su dispositivo. De manera predeterminada, no hay una versión definida.

- Certificado de usuario

  Seleccione uno de los siguientes valores:

  - **Instalado**. Una regla de movimiento de dispositivos solo se aplica a dispositivos móviles con un certificado para dispositivos móviles.
  - **Sin instalar**. La regla de movimiento de dispositivos solo se aplica a dispositivos móviles sin un certificado para dispositivos móviles.
  - **Ningún valor seleccionado**. La condición no se aplica.

- Compilación del sistema operativo

  Este parámetro solo es válido para sistemas operativos Windows.

  Puede indicar si el número de compilación del sistema operativo seleccionado deberá ser igual, anterior o posterior al valor introducido. También puede configurar la búsqueda de una regla de movimiento para todos los números de compilación, excepto el especificado.

- Número de versión del sistema operativo

  Este parámetro solo es válido para sistemas operativos Windows.

  Puede especificar si el sistema operativo seleccionado debe tener un número de versión igual, anterior o posterior. También puede configurar una regla de movimiento de dispositivos para todos los números de versión excepto el especificado.

## Pestaña Máquinas virtuales

En esta pestaña puede configurar la búsqueda de dispositivos según sean dispositivos virtuales o parte de la infraestructura de escritorio virtual (VDI):

- Esta es una máquina virtual

  En la lista desplegable se puede seleccionar lo siguiente:
  - **N/D**. La condición no se aplica.
  - **No**. Mover dispositivos que no son máquinas virtuales.
  - **Sí**. Mover dispositivos que son máquinas virtuales.

- **Tipo de máquina virtual**

- Parte de la infraestructura de escritorio virtual

  En la lista desplegable se puede seleccionar lo siguiente:
  - **N/D**. La condición no se aplica.
  - **No**. Mover dispositivos que no forman parte de la VDI.
  - **Sí**. Mover de dispositivos que son parte de la VDI.

## Pestaña Controlador de dominio

En esta pestaña, puede especificar que es necesario mover los dispositivos incluidos en la unidad organizativa del dominio. También puede mover dispositivos de todas las unidades organizativas secundarias de la unidad organizativa del dominio especificado:

- **El dispositivo está incluido en la siguiente unidad organizativa**

  Si esta opción está habilitada, se aplica una regla de movimiento de dispositivos a los dispositivos de la unidad organizativa del dominio especificada en la lista que hay debajo de la opción.

  Esta opción está deshabilitada de forma predeterminada.

- **Incluir unidades organizativas secundarias**

  Si habilita esta opción, la selección incluirá los dispositivos de todas las unidades organizativas secundarias de la unidad organizativa del dominio especificado.

  Esta opción está deshabilitada de forma predeterminada.

- **Mover los dispositivos de unidades secundarias a subgrupos correspondientes**
- **Crear subgrupos correspondientes a contenedores de dispositivos recién detectados**
- **Eliminar subgrupos no presentes en el dominio**
- **Incluir el dispositivo en el siguiente grupo de seguridad de dominio**

  Si esta opción está habilitada, se aplica una regla de movimiento de dispositivos a los dispositivos del grupo de seguridad de dominio especificados en la lista que hay debajo de la opción.

  Esta opción está deshabilitada de forma predeterminada.

## Pestaña Segmentos de nube

En esta pestaña, puede especificar que es necesario mover los dispositivos que pertenecen a segmentos de la nube específicos:

- **El dispositivo se encuentra en un segmento de la nube**

  Si selecciona esta opción, una regla de movimiento de dispositivos se aplica a los dispositivos cliente que pertenecen a un segmento de la nube. Puede seleccionar el segmento de nube requerido hasta una subred en la lista que hay debajo de la opción.

  La opción está desactivada de forma predeterminada.

- **Incluir objetos secundarios**

  Si selecciona esta opción, se aplica una regla de movimiento de dispositivos no solo al segmento de nube seleccionado, sino también a los objetos secundarios de este segmento.

  La opción está desactivada de forma predeterminada.

- **Mover los dispositivos de objetos anidados a subgrupos correspondientes**
- **Crear subgrupos correspondientes a contenedores de dispositivos recién detectados**
- **Eliminar subgrupos para los que no se encuentre coincidencia en los segmentos de nube**
- Dispositivo encontrado mediante API

  La lista desplegable le permite operar con el hecho de que el dispositivo pueda detectarse con las herramientas provistas por una API.

  - **AWS**. El dispositivo se descubre mediante la API de AWS, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de AWS.
  - **Azure**. El dispositivo se descubre mediante la API de Azure, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de Azure.
  - **Google Cloud.** El dispositivo se descubre utilizando la API de Google, es decir, el dispositivo está en el entorno de Google Cloud.
  - **No**. El dispositivo no se puede detectar con la API de AWS, Azure o Google (o bien el dispositivo no se encuentra en el entorno de nube, o bien sí está en el entorno de nube, pero, por algún motivo, no se lo puede detectar con una API).
  - **Ningún valor.** Esta condición no se aplica.

## Sobre clústeres y conjuntos de servidores

Kaspersky Security Center admite la tecnología de clúster. Si el Agente de red envía información al Servidor de administración que confirma que la aplicación instalada en un dispositivo cliente forma parte de una matriz de servidores, el dispositivo cliente se convierte en un nodo del clúster.

Si un grupo de administración contiene clústeres o conjuntos de servidores, la página **Dispositivos administrados** muestra dos pestañas: una para dispositivos individuales y otra para clústeres y conjuntos de servidores. Una vez que los dispositivos administrados se detectan como nodos de clúster, el clúster se agrega como un objeto individual a la pestaña **Clústeres y conjuntos de servidores**.

Los nodos de los clústeres o conjuntos de servidores se enumeran en la pestaña **Dispositivos**, junto con otros dispositivos administrados. Puede ver las propiedades de los nodos como dispositivos individuales y llevar a cabo otras operaciones, pero no puede eliminar un nodo de clúster ni moverlo a otro grupo de administración por separado de su clúster. Solo puede eliminar o mover un clúster completo.

Puede realizar las siguientes operaciones con clústeres o conjuntos de servidores:

- Ver las propiedades
- Mover el clúster o conjunto de servidores a otro grupo de administración

  Cuando mueve un clúster o un conjunto de servidores a otro grupo, todos sus nodos se mueven con él, porque un clúster y cualquiera de sus nodos siempre pertenecen al mismo grupo de administración.

- Eliminar

  Es razonable eliminar un clúster o un conjunto de servidores solo cuando el clúster o conjunto de servidores ya no existe en la red de la organización. Si un clúster aún está visible en su red y el Agente de red y la aplicación de seguridad de Kaspersky todavía están instalados en los nodos del clúster, Kaspersky Security Center devuelve el clúster eliminado y sus nodos a la lista de dispositivos administrados de manera automática.

# Propiedades de un clúster o conjunto de servidores

*Para ver la configuración de un clúster o conjunto de servidores:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados** → **Clústeres y conjuntos de servidores**.

   Se muestra la lista de clústeres y conjuntos de servidores.

2. Haga clic en el nombre del clúster o conjunto de servidores requerido.

Se muestra la ventana de propiedades del clúster o conjunto de servidores seleccionado.

## General

La sección **General** muestra información general sobre el clúster o conjunto de servidores. La información se basa en los datos recibidos durante la última sincronización de los nodos del clúster con el Servidor de administración.

- **Nombre**
- **Descripción**
- Dominio de Windows

  Dominio o grupo de trabajo de Windows, que contiene el clúster o conjunto de servidores.

- Nombre NetBIOS

  Nombre de red de Windows del clúster o conjunto de servidores.

- Nombre DNS

  Nombre del dominio DNS del clúster o conjunto de servidores.

### Tareas

La pestaña **Tareas** permite administrar las tareas del clúster o conjunto de servidores. Utilice esta sección para crear tareas nuevas, ver la lista de tareas existentes, ver los resultados de ejecución de las tareas e iniciar, detener, eliminar y reconfigurar las tareas existentes. Las tareas enumeradas se relacionan con la aplicación de seguridad de Kaspersky instalada en los nodos del clúster. Kaspersky Security Center recibe la lista de tareas y los detalles del estado de las tareas de los nodos del clúster. Si no se puede establecer una conexión, no se mostrará ningún estado.

### Nodos

Esta pestaña muestra una lista de nodos incluidos en el clúster o conjunto de servidores. Puede hacer clic en el nombre de un nodo para ver la ventana de propiedades del dispositivo.

### Aplicación de Kaspersky

La ventana de propiedades también puede contener pestañas adicionales con información y configuraciones relacionadas con la aplicación de seguridad de Kaspersky instalada en los nodos del clúster.

## Ver y configurar las acciones para dispositivos inactivos

Puede recibir una notificación si se detecta que los dispositivos cliente de un grupo están inactivos. También puede hacer que esos dispositivos se eliminen automáticamente.

*Para ver o configurar las acciones que se llevan a cabo cuando los dispositivos de un grupo están inactivos:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Jerarquía de grupos**.
2. Haga clic en el nombre del grupo de administración de su interés.

   Se abrirá la ventana de propiedades del grupo de administración.
3. En la ventana de propiedades, vaya a la pestaña **Configuración**.
4. En la sección **Herencia**, active o desactive las siguientes opciones:

   - **Heredar del grupo primario**

     La configuración de la sección se heredará del grupo primario al que pertenezca el dispositivo cliente. Si esta opción está habilitada, los ajustes de la sección **Actividad de los dispositivos en la red** no se podrán modificar.

     Para que esta opción esté disponible, el grupo de administración debe tener un grupo primario.

     Esta opción está activada de forma predeterminada.

   - **Forzar la herencia de configuración en los grupos secundarios**

     Los valores de configuración se propagarán a los grupos secundarios. Los ajustes correspondientes estarán bloqueados en las propiedades de esos grupos.

     Esta opción está deshabilitada de forma predeterminada.

5. En la sección **Actividad de los dispositivos**, active o deshabilite las siguientes opciones:

- **Notificar al administrador si el dispositivo ha estado inactivo por más de (días)**

  Cuando esta opción está habilitada y se detecta que un dispositivo ha estado inactivo, el administrador recibe una notificación. Puede especificar el intervalo de tiempo que se deja pasar antes de que se cree el evento **El dispositivo ha estado inactivo en la red por mucho tiempo**. El intervalo de tiempo por defecto es de 7 días.

  Esta opción está activada de forma predeterminada.

- **Eliminar el dispositivo del grupo si ha estado inactivo por más de (días)**

  Si esta opción está habilitada, puede especificar el intervalo de tiempo que se deja pasar antes de que el dispositivo se elimine del grupo automáticamente. El intervalo de tiempo por defecto es de 60 días.

  Esta opción está activada de forma predeterminada.

6. Haga clic en **Guardar**.

Se guardarán y aplicarán los cambios.

## Acerca de los estados de los dispositivos

Kaspersky Security Center le asigna un estado a cada dispositivo administrado. El estado asignado depende de que se cumplan las condiciones definidas por el usuario. En algunos casos, al asignar un estado a un dispositivo, Kaspersky Security Center tiene en cuenta el indicador de visibilidad del dispositivo en la red (consulte la tabla a continuación). Por ejemplo, si a un dispositivo administrado se le asigna el estado *Crítico* por cumplirse la condición *Las bases de datos están desactualizadas*, y luego se activa el indicador de visibilidad para ese dispositivo, el estado del dispositivo cambia a *Sin inconvenientes*. Si Kaspersky Security Center no encuentra un dispositivo en la red en un plazo de dos horas, el indicador de visibilidad del dispositivo se establece en *No visible*.

Los estados son los siguientes:

- *Crítico* o *Crítico/Visible*
- *Advertencia* o *Advertencia/Visible*
- *Sin inconvenientes* o *Sin inconvenientes/Visible*

En la siguiente tabla, se enumeran las condiciones predeterminadas que se deben cumplir para que se asignen los estados *Crítico* o *Advertencia* a un dispositivo, con todos los valores posibles.

Condiciones para que se asigne un estado a un dispositivo

| Condición | Descripción de la condición | Valores disponibles |
|---|---|---|
| La aplicación de seguridad no está instalada | El Agente de red está instalado en el dispositivo, pero no hay una aplicación de seguridad instalada. | • Interruptor activado.<br>• Interruptor desactivado. |
| Se detectaron demasiados virus | Una tarea de detección de virus (por ejemplo, la tarea *Análisis antimalware*) detectó en el dispositivo una cantidad de virus superior al valor especificado. | Más de 0. |

| Condición | Descripción de la condición | Valores disponibles |
|---|---|---|
| El nivel de protección en tiempo real difiere del nivel establecido por el administrador | El dispositivo es visible en la red, pero el nivel de la protección en tiempo real no se corresponde con el que el administrador configuró (en la condición) para el estado del dispositivo. | • Detenida.<br>• En pausa.<br>• En ejecución. |
| No se ha realizado un análisis antimalware en mucho tiempo | El dispositivo está visible en la red y tiene instalada una aplicación de seguridad, pero la tarea *Análisis antimalware* no se ha ejecutado en el intervalo de tiempo especificado. Esta condición se aplica solo a los dispositivos que se agregaron al menos siete días antes a la base de datos del Servidor de administración. | Más de 1 día. |
| Las bases de datos están desactualizadas | El dispositivo es visible en la red y tiene instalada una aplicación de seguridad, pero sus bases de datos antivirus no se han actualizado en el período de tiempo especificado. Esta condición se aplica solo a los dispositivos que se agregaron al menos un día antes a la base de datos del Servidor de administración. | Más de 1 día. |
| Sin conexión desde hace mucho tiempo | El Agente de red está instalado en el dispositivo, pero el dispositivo está apagado y no se ha conectado a un Servidor de administración durante el período de tiempo especificado. | Más de 1 día. |
| Se han detectado amenazas activas | El número de objetos no procesados en la carpeta **Amenazas activas** supera el valor especificado. | Más de 0 elementos. |
| Se debe reiniciar el dispositivo | El dispositivo es visible en la red, pero una aplicación requiere que el dispositivo se reinicie por más tiempo que el intervalo de tiempo especificado y por una de las razones seleccionadas. | Más de 0 minutos. |
| Hay aplicaciones incompatibles instaladas | El dispositivo es visible en la red, pero, al hacer un inventario de software a través del Agente de red, se detectaron aplicaciones incompatibles instaladas en el dispositivo. | • Interruptor desactivado.<br>• Interruptor activado. |
| Se detectaron vulnerabilidades de software | El dispositivo es visible en la red y tiene instalado el Agente de red, pero la tarea *Buscar vulnerabilidades y actualizaciones requeridas* ha encontrado aplicaciones instaladas en el dispositivo que tienen vulnerabilidades con el nivel de gravedad especificado. | • Crítico.<br>• Alto.<br>• Medio.<br>• Ignorar si la vulnerabilidad no se puede reparar.<br>• Ignorar si hay una actualización asignada para instalarse. |
| Licencia caducada | El dispositivo es visible en la red, pero la licencia ha caducado. | • Interruptor desactivado.<br>• Interruptor activado. |
| La licencia está por caducar | El dispositivo es visible en la red, pero la licencia instalada en el mismo caduca en menos días que el número de días especificado. | Menos de 0 días. |
| La búsqueda de actualizaciones de Windows Update no se ha realizado en mucho tiempo | El dispositivo es visible en la red, pero la tarea *Realizar la sincronización de Windows Update* no se ejecutó durante el intervalo de tiempo especificado. | Más de 1 día. |

| Condición | Descripción de la condición | Valores disponibles |
|---|---|---|
| Estado de cifrado no válido | El Agente de red está instalado en el dispositivo, pero el resultado del cifrado del dispositivo es igual al valor especificado. | • No cumple con la directiva porque el usuario no dio su consentimiento (solo para dispositivos externos).<br>• No cumple con la directiva debido a un error.<br>• Se debe reiniciar el dispositivo al aplicar la directiva.<br>• No se ha especificado una directiva de cifrado.<br>• No compatible.<br>• Al aplicar la directiva. |
| La configuración del dispositivo móvil no cumple con la directiva | Los ajustes del dispositivo móvil no son los que se encontraron en la directiva de Kaspersky Endpoint Security para Android durante el chequeo de reglas de cumplimiento normativo. | • Interruptor desactivado.<br>• Interruptor activado. |
| Problemas de seguridad no procesados detectados | Se han encontrado problemas de seguridad sin procesar en el dispositivo. Los problemas de seguridad se pueden crear manualmente por el administrador o automáticamente por las aplicaciones de Kaspersky administradas que se han instalado en el dispositivo cliente. | • Interruptor desactivado.<br>• Interruptor activado. |
| Estado del dispositivo definido por la aplicación | El estado del dispositivo es definido por la aplicación administrada.<br>Los dispositivos administrados pueden tener un estado determinado por las aplicaciones administradas, independientemente de los parámetros de Kaspersky Security Center. Después de que este estado devuelve uno de los estados definidos por Kaspersky Security Center, el Servidor de administración asigna a un dispositivo administrado el estado más crítico de los devueltos por la aplicación administrada y asignados por el Servidor de administración. Los estados definidos por la administración de aplicaciones tienen descripciones transferidas por las aplicaciones administradas. Puede ver las descripciones en la lista de dispositivos administrados, en la columna **Descripción del estado**. | • Interruptor desactivado.<br>• Interruptor activado. |
| El dispositivo no tiene espacio en el disco | El espacio libre en el disco del dispositivo es inferior al valor especificado o el dispositivo no se pudo sincronizar con el Servidor de administración. Los estados *Crítico* o *Advertencia* cambiarán por el estado *Sin inconvenientes* cuando el dispositivo se sincronice correctamente con el Servidor de administración y el espacio libre en el dispositivo supere o iguale el valor especificado. | Más de 0 MB. |
| El dispositivo ha cambiado a no administrado | Durante el descubrimiento de dispositivos, el dispositivo se reconoció como visible en la red, pero hubo más de tres intentos de sincronizar el dispositivo con el Servidor de administración que terminaron con un error. | • Interruptor desactivado.<br>• Interruptor activado. |
| Protección deshabilitada | El dispositivo es visible en la red, pero la aplicación de seguridad del dispositivo ha estado deshabilitada por un tiempo superior al especificado.<br>En este caso, el estado de la aplicación de seguridad es *detenida* o *error*, y difiere del siguiente: *iniciada*, *en ejecución* o *suspendida*. | Más de 0 minutos. |
| La aplicación de seguridad no está en ejecución | El dispositivo es visible en la red y tiene instalada una aplicación de seguridad, pero esa aplicación no se está ejecutando. | • Interruptor desactivado.<br>• Interruptor activado. |

Kaspersky Security Center permite que usted configure la conmutación automática del estado de un dispositivo en un grupo de administración cuando las condiciones especificadas se cumplen. El estado del dispositivo cliente puede hacerse pasar a *Crítico* o *Advertencia* si se cumplen las condiciones configuradas. Si no se cumplen estas condiciones, el dispositivo cliente toma el estado *Sin inconvenientes*.

Cada estado puede corresponderse con distintos valores de una misma condición. De forma predeterminada, por ejemplo, cuando la condición **Las bases de datos están desactualizadas** tiene el valor **Más de 3 días**, se asigna el estado *Advertencia* al dispositivo cliente; si el valor es **Más de 7 días**, se asigna el estado *Crítico*.

Si actualiza Kaspersky Security Center desde la versión anterior, los valores de la condición **Las bases de datos están desactualizadas** para asignar el estado a *Crítico* o *Advertencia* no cambian.

## Configurar cambios de estado para los dispositivos

Puede cambiar las condiciones bajo las cuales se le asignan los estados *Crítico* o *Advertencia* a un dispositivo.

*Para habilitar el cambio de estado a Crítico para los dispositivos:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Jerarquía de grupos**.
2. En la lista de grupos que se abre, haga clic en el vínculo con el nombre del grupo que contenga los dispositivos para los que desee modificar el cambio de estado.
3. En la ventana de las propiedades que se abre, seleccione la pestaña **Estado del dispositivo**.
4. En el panel izquierdo, seleccione **Crítico**.
5. En el panel derecho, en la sección **Fijar en Crítico si esto se cumple**, habilite la condición bajo la cual el estado de un dispositivo cambiará a *Crítico*.

   Solo podrá modificar los ajustes que no estén bloqueados en la directiva primaria.

6. En la lista, seleccione el botón de opción ubicado junto a la condición.
7. En la esquina superior izquierda de la lista, haga clic en el botón **Editar**.
8. Configure el valor necesario para la condición seleccionada.

   No es posible configurar valores para todas las condiciones.
9. Haga clic en **Aceptar**.

Cuando se cumplan las condiciones especificadas, se asignará el estado *Crítico* al dispositivo administrado.

*Para habilitar el cambio de estado a Advertencia para los dispositivos:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Jerarquía de grupos**.
2. En la lista de grupos que se abre, haga clic en el vínculo con el nombre del grupo que contenga los dispositivos para los que desee modificar el cambio de estado.
3. En la ventana de las propiedades que se abre, seleccione la pestaña **Estado del dispositivo**.
4. En el panel izquierdo, seleccione **Advertencia**.

5. En el panel derecho, en la sección **Fijar en Advertencia si esto se cumple**, habilite la condición que hará que el estado de un dispositivo cambie a *Advertencia*.

   Solo podrá modificar los ajustes que no estén bloqueados en la directiva primaria.

6. En la lista, seleccione el botón de opción ubicado junto a la condición.
7. En la esquina superior izquierda de la lista, haga clic en el botón **Editar**.
8. Configure el valor necesario para la condición seleccionada.

   No es posible configurar valores para todas las condiciones.

9. Haga clic en **Aceptar**.

Cuando se cumplan las condiciones especificadas, se asignará el estado *Advertencia* al dispositivo administrado.

## Conexión remota al escritorio de un dispositivo cliente

El administrador puede obtener acceso remoto al escritorio de un dispositivo cliente a través de un Agente de red instalado en el dispositivo cliente. El Agente de red permite conectarse incluso si el dispositivo cliente tiene cerrados los puertos TCP y UDP.

Al establecer la conexión con el dispositivo, el administrador obtiene acceso completo a la información almacenada en este dispositivo, de manera que puede administrar las aplicaciones instaladas en él.

Las conexiones remotas deben estar permitidas por el sistema operativo del dispositivo administrado al que pretenda acceder. En Windows 10, por ejemplo, debe estar habilitada la opción **Permitir conexiones de Asistencia remota a este equipo**, que se encuentra en **Panel de control** → **Sistema y seguridad** → **Sistema** → **Configuración de Acceso remoto**. Si tiene una licencia para la característica Administración de vulnerabilidades y parches, puede habilitar esta opción por la fuerza al conectarse al dispositivo administrado. Si no tiene una licencia para esta función, habilite la opción de manera local en el dispositivo administrado. No podrá establecer una conexión remota si esta opción está deshabilitada.

Para conectarse a un dispositivo remoto, debe contar con dos utilidades:

- La utilidad klsctunnel, desarrollada por Kaspersky. Este programa debe estar almacenado en la estación de trabajo del administrador. Se utiliza para conectar el Servidor de administración con el dispositivo cliente a través de un túnel.

  Kaspersky Security Center permite hacer túneles de conexión TCP desde la Consola de administración mediante el Servidor de administración y luego mediante el Agente de red a un puerto especificado en un dispositivo administrado. Gracias a este túnel, una aplicación cliente instalada en el mismo dispositivo que la Consola de administración puede conectarse a un puerto TCP de un dispositivo administrado incluso si no existe una vía de conexión directa entre la Consola de administración y ese dispositivo administrado.

  La conexión entre el Servidor de administración y el dispositivo cliente remoto se debe hacer pasar por un túnel cuando el puerto que se utiliza para conectarse al Servidor de administración no está disponible en el dispositivo. El puerto del dispositivo podría no estar disponible en estos casos:

  - el dispositivo remoto está conectado a una red local en la que se utiliza el mecanismo NAT;
  - el dispositivo remoto está en la misma red local que el Servidor de administración, pero el puerto se ha cerrado con un firewall.

- El componente Conexión a Escritorio remoto, que forma parte de Microsoft Windows. La conexión con el escritorio remoto se establece a través de mstsc.exe, una utilidad que viene incluida en Windows, conforme a los ajustes de la utilidad.

  Si se conecta a la sesión de escritorio remoto establecida por un usuario, lo hará sin que el usuario lo sepa. Una vez que el administrador se conecta a la sesión, el usuario del dispositivo queda desconectado de la sesión sin notificación previa.

*Para conectarse al escritorio de un dispositivo cliente:*

1. En la Consola de administración basada en MMC, abra el menú contextual del Servidor de administración y seleccione **Propiedades**.
2. En la ventana de propiedades del Servidor de administración, vaya a **Configuración de conexión del Servidor de administración → Puertos de conexión**.
3. Verifique que la opción **Abrir puerto de RDP para Kaspersky Security Center Web Console** esté habilitada.
4. En Kaspersky Security Center Web Console, vaya a **Activos (dispositivos) → Dispositivos administrados**.
5. En el campo **Ruta actual** ubicado sobre la lista de dispositivos administrados, haga clic en el vínculo de la ruta.
6. En el panel que se abre del lado izquierdo, seleccione el grupo de administración que contenga el dispositivo al que desee obtener acceso.
7. Active la casilla de verificación ubicada junto al nombre del dispositivo al que desee acceder.
8. Haga clic en el botón **Conectar con escritorio remoto**.

   Se abre la ventana Escritorio remoto (solo Windows).

9. Active la opción **Permitir conexión de escritorio remota en dispositivo administrado**. En este caso, la conexión se establecerá incluso si las conexiones remotas están actualmente prohibidas en la configuración del sistema operativo del dispositivo administrado.

   Esta opción solo está disponible si tiene una licencia para la función Administración de vulnerabilidades y parches.

10. Haga clic en el botón **Descargar** para descargar la utilidad klsctunnel.

11. Haga clic en el botón **Copiar al portapapeles** para copiar el contenido del campo de texto. El contenido del campo es un objeto binario (denominado "BLOB", por el nombre de este tipo de objeto en inglés). El objeto contiene los parámetros que se necesitan para establecer la conexión entre el Servidor de administración y el dispositivo administrado.

    Los BLOB tienen una validez de tres minutos. Si el suyo caduca, vuelva a abrir la ventana Escritorio remoto (solo Windows) para generar un nuevo BLOB.

12. Ejecute la utilidad klsctunnel.

    Se abre la ventana de la utilidad.

13. En el campo de texto, pegue el contenido que copió en el paso anterior.

14. Si utiliza un servidor proxy, active la casilla **Usar servidor proxy** y especifique los ajustes de conexión del servidor proxy.

15. Haga clic en el botón **Abrir puerto**.

    Se abre la ventana de inicio de sesión de Conexión a Escritorio remoto.

16. Especifique las credenciales de la cuenta con la que haya iniciado sesión en Kaspersky Security Center Web Console.

17. Haga clic en el botón **Conectar**.

Una vez que se establezca la conexión con el dispositivo, tendrá acceso al escritorio a través de la ventana Conexión a Escritorio remoto de Microsoft Windows.

## Conectarse a un dispositivo a través de Windows Desktop Sharing

El administrador puede obtener acceso remoto al escritorio de un dispositivo cliente a través de un Agente de red instalado en el dispositivo cliente. El Agente de red permite conectarse incluso si el dispositivo cliente tiene cerrados los puertos TCP y UDP.

El administrador se puede conectar a una sesión existente en un dispositivo cliente sin desconectar al usuario de esta sesión. En tal caso, el acceso al escritorio se comparte entre el administrador y el usuario que inició la sesión.

Para conectarse a un dispositivo remoto, debe contar con dos utilidades:

- La utilidad klsctunnel, desarrollada por Kaspersky. Este programa debe estar almacenado en la estación de trabajo del administrador. Se utiliza para conectar el Servidor de administración con el dispositivo cliente a través de un túnel.

  Kaspersky Security Center permite hacer túneles de conexión TCP desde la Consola de administración mediante el Servidor de administración y luego mediante el Agente de red a un puerto especificado en un dispositivo administrado. Gracias a este túnel, una aplicación cliente instalada en el mismo dispositivo que la Consola de administración puede conectarse a un puerto TCP de un dispositivo administrado incluso si no existe una vía de conexión directa entre la Consola de administración y ese dispositivo administrado.

  La conexión entre el Servidor de administración y el dispositivo cliente remoto se debe hacer pasar por un túnel cuando el puerto que se utiliza para conectarse al Servidor de administración no está disponible en el dispositivo. El puerto del dispositivo podría no estar disponible en estos casos:

  - el dispositivo remoto está conectado a una red local en la que se utiliza el mecanismo NAT;
  - el dispositivo remoto está en la misma red local que el Servidor de administración, pero el puerto se ha cerrado con un firewall.

- Windows Desktop Sharing. Al conectarse con una sesión existente del escritorio remoto, el usuario de la sesión en el dispositivo recibe una solicitud de conexión del administrador. No hay información acerca de la actividad remota del dispositivo, y los resultados se guardarán en informes creados por Kaspersky Security Center.

  El administrador puede configurar una auditoría de la actividad del usuario en un dispositivo cliente remoto. Durante la auditoría, la aplicación guarda información sobre los archivos del dispositivo cliente que el administrador haya abierto o modificado.

Para que pueda conectarse al escritorio de un dispositivo cliente a través de Windows Desktop Sharing, se deben cumplir las siguientes condiciones:

- La estación de trabajo del administrador debe tener Microsoft Windows Vista o una versión de Windows posterior. El tipo de sistema operativo del dispositivo que alberga al Servidor de administración no impone restricciones con respecto a la conexión a través de Windows Desktop Sharing.

  Para determinar si la característica Windows Desktop Sharing está disponible en su edición de Windows, verifique que la clave CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} esté presente en el registro de Windows.

- El dispositivo cliente debe tener Microsoft Windows Vista o una versión de Windows posterior.

- Kaspersky Security Center usa una licencia para la Administración de vulnerabilidades y parches.

*Para conectarse al escritorio de un dispositivo cliente a través de Escritorio compartido de Windows:*

1. En la Consola de administración basada en MMC, abra el menú contextual del Servidor de administración y seleccione **Propiedades**.
2. En la ventana de propiedades del Servidor de administración, vaya a **Configuración de conexión del Servidor de administración** → **Puertos de conexión**.
3. Verifique que la opción **Abrir puerto de RDP para Kaspersky Security Center Web Console** esté habilitada.
4. En Kaspersky Security Center Web Console, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.
5. En el campo **Ruta actual** ubicado sobre la lista de dispositivos administrados, haga clic en el vínculo de la ruta.

6. En el panel que se abre del lado izquierdo, seleccione el grupo de administración que contenga el dispositivo al que desee obtener acceso.

7. Active la casilla de verificación ubicada junto al nombre del dispositivo al que desee acceder.

8. Haga clic en el botón **Windows Desktop Sharing**.

   Se abre el asistente de Windows Desktop Sharing.

9. Haga clic en el botón **Descargar** para obtener la utilidad klsctunnel. Espere a que se complete la descarga.

   Si ya tiene el archivo de la utilidad, omita este paso.

10. Haga clic en el botón **Siguiente**.

11. Elija una sesión abierta en el dispositivo al que desee conectarse. A continuación, haga clic en el botón **Siguiente**.

12. En el dispositivo de destino, se abrirá un cuadro de diálogo para que el usuario autorice la sesión de escritorio compartido. La sesión no comenzará sin el consentimiento del usuario.

    Una vez que el usuario del dispositivo confirma la sesión de escritorio compartido, se abre la siguiente página del Asistente.

13. Haga clic en el botón **Copiar al portapapeles** para copiar el contenido del campo de texto. El contenido del campo es un objeto binario (denominado "BLOB", por el nombre de este tipo de objeto en inglés). El objeto contiene los parámetros que se necesitan para establecer la conexión entre el Servidor de administración y el dispositivo administrado.

    > Los BLOB tienen una validez de tres minutos. Si su BLOB caduca, genere uno nuevo.

14. Ejecute la utilidad klsctunnel.

    Se abre la ventana de la utilidad.

15. En el campo de texto, pegue el contenido que copió en el paso anterior.

16. Si utiliza un servidor proxy, active la casilla **Usar servidor proxy** y especifique los ajustes de conexión del servidor proxy.

17. Haga clic en el botón **Abrir puerto**.

La sesión de escritorio compartido se abre en una nueva ventana. Si necesita interactuar con el dispositivo, haga clic en el ícono de menú (  ) ubicado en la esquina superior izquierda de la ventana y seleccione **Modo interactivo**.

## Selecciones de dispositivos

Las *selecciones de dispositivos* son una herramienta para filtrar dispositivos de acuerdo con condiciones específicas. Puede usar selecciones de dispositivos para administrar varios dispositivos a la vez y, por ejemplo, moverlos de un grupo a otro o ver un informe que trate únicamente sobre ellos.

Kaspersky Security Center proporciona una amplia gama de *selecciones predefinidas* (por ejemplo, **Dispositivos con estado Crítico**, **Protección deshabilitada**, **Se han detectado amenazas activas**). Las selecciones predefinidas no se pueden eliminar. De ser necesario, puede crear y configurar selecciones adicionales, llamadas *selecciones definidas por el usuario*.

En una selección definida por el usuario, se puede determinar el alcance de la búsqueda y seleccionar todos los dispositivos, los dispositivos administrados o los dispositivos no asignados. Los parámetros de búsqueda se especifican en las condiciones. Una selección de dispositivos puede tener varias condiciones con diferentes parámetros de búsqueda. Puede, por ejemplo, crear dos condiciones y especificar intervalos IP diferentes en cada una de ellas. Una selección con varias condiciones muestra los dispositivos que cumplen con cualquiera de esas condiciones. Por el contrario, los parámetros de búsqueda especificados en una condición se superponen. Si una condición especifica tanto un intervalo IP como el nombre de una aplicación instalada, se mostrarán únicamente los dispositivos que tengan asignada una dirección IP de ese intervalo y que tengan instalada esa aplicación.

## Ver la lista de dispositivos de una selección de dispositivos

Kaspersky Security Center Cloud Console le permite ver la lista de dispositivos desde una selección de dispositivos.

*Para ver la lista de dispositivos de una selección de dispositivos:*

1. En el menú principal, vaya a las secciones **Activos (dispositivos)** → **Selecciones de dispositivos** o **Descubrimiento y despliegue** → **Selecciones de dispositivos**.
2. En la lista de selecciones, haga clic en el nombre de la selección de dispositivos.

   La página muestra una tabla con información sobre los dispositivos incluidos en la selección de dispositivos.
3. Puede hacer lo siguiente para agrupar y filtrar los datos que conforman la tabla de dispositivos:

   - Haga clic en el ícono de configuración ( ⚙ ) y seleccione las columnas que se deban mostrar en la tabla.
   - Haga clic en el ícono de filtro ( ▽ ) y, en el menú que se abrirá, defina el criterio de filtrado.

     Se mostrará la tabla de dispositivos filtrada.

Puede seleccionar uno o varios dispositivos en la selección de dispositivos y hacer clic en el botón **Nueva tarea** para crear una tarea que se aplicará a estos dispositivos.

Para mover los dispositivos seleccionados de la selección de dispositivos a otro grupo de administración, haga clic en el botón **Mover a un grupo** y luego seleccione el grupo de administración de destino.

## Crear una selección de dispositivos

*Para crear una selección de dispositivos:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Selecciones de dispositivos**.

   Se muestra una página con una lista de selecciones de dispositivos.
2. Haga clic en el botón **Agregar**.

   Se abre la ventana **Configuración de la selección de dispositivos**.
3. Escriba el nombre de la nueva selección.

4. Especifique el grupo que contiene los dispositivos que desea incluir en la selección de dispositivos:

   - **Buscar cualquier dispositivo**: Buscar dispositivos que cumplan con los criterios de selección y que estén incluidos en el grupo **Dispositivos administrados** o **Dispositivos no asignados**.
   - **Buscar dispositivos administrados**: Buscar dispositivos que cumplan con los criterios de selección y que estén incluidos en el grupo **Dispositivos administrados**.
   - **Buscar dispositivos no asignados**: Buscar dispositivos que cumplan con los criterios de selección y que estén incluidos en el grupo **Dispositivos no asignados**.

   Puede habilitar la casilla de verificación **Incluir datos de Servidores de administración secundarios** para habilitar la búsqueda de dispositivos que cumplan con los criterios de selección y que estén administrados por Servidores de administración secundarios.

5. Haga clic en el botón **Agregar**.
6. En la ventana que se abre, especifique las condiciones que deben cumplirse para incluir los dispositivos en esta selección y, a continuación, haga clic en el botón **Aceptar**.
7. Haga clic en el botón **Guardar**.

La selección de dispositivos se crea y se agrega a la lista de selecciones de dispositivos.

## Configurar una selección de dispositivos

*Para configurar una selección de dispositivos:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Selecciones de dispositivos**.

   Se muestra una página con una lista de selecciones de dispositivos.

2. Elija la selección de dispositivos definida por el usuario pertinente y haga clic en el botón **Propiedades**.

   Se abre la ventana **Configuración de la selección de dispositivos**.

3. En la pestaña **General**, haga clic en el vínculo **Nueva condición**.
4. Especifique las condiciones que deban cumplirse para que un dispositivo se incluya o no en la selección.
5. Haga clic en el botón **Guardar**.

El cambio se aplica y se guarda.

A continuación, se presentan descripciones de las condiciones para asignar dispositivos a una selección. Las condiciones se combinan usando el operador lógico OR: la selección incluirá dispositivos que cumplan con, al menos, una de las condiciones de la lista.

### General

En la sección **General**, puede cambiar el nombre de una condición de la selección y especificar si esa condición se debería invertir:

Invertir condición de selección

Esta opción está deshabilitada de forma predeterminada.

Si habilita esta opción, la condición elegida se aplicará a la inversa. La selección incluirá todos los dispositivos que no cumplan con la condición.

El siguiente ejemplo muestra la lógica del trabajo de inversión:

- **Condición**: en su dispositivo, hay un sistema operativo de tipo Linux y con número de compilación 00.0.000.
- **Condición invertida**: en su dispositivo, existe un sistema operativo con NOT (el tipo Linux y el número de compilación 00.0.000), lo que es equivalente a lo siguiente:

  Hay un sistema operativo con el tipo NOT Linux O el número de compilación NOT 00.0.000.

Por lo tanto, la selección incluirá los dispositivos con un sistema operativo, por ejemplo, del tipo Windows y el número de compilación 00.0.000, o del tipo Linux y cualquier número de compilación que no sea 00.0.000.

## Infraestructura de red

En la sección **Red**, puede especificar los criterios que serán usados para incluir dispositivos en la selección según sus datos de la red:

- Nombre del dispositivo

  Nombre de red de Windows (nombre NetBIOS) del dispositivo, o la dirección IPv4 o IPv6.

- Dominio

  Muestra todos los dispositivos incluidos en el dominio de Windows especificado.

- Grupo de administración

  Muestra los dispositivos incluidos en el grupo de administración especificado.

- **Descripción**

  Texto ubicado en el campo **Descripción** de la sección **General** dentro de la ventana de propiedades del dispositivo.

  Para describir el texto del campo **Descripción**, puede utilizar los siguientes caracteres:

  - Dentro de una palabra:

    - *****. Sustituye una cadena de cualquier largo (es decir, con cualquier número de caracteres).

    **Ejemplo**:

    Para describir palabras como **Servidor** o **Servidores**, puede ingresar **Servidor***.

    - **?.** Sustituye un carácter individual.

    **Ejemplo**:

    Para describir palabras como **Window** o **Windows**, puede ingresar **Windo?**.

    La consulta no puede comenzar con un asterisco (*****) ni con un signo de interrogación (**?**).

  - Para encontrar varias palabras:

    - Espacio. Muestra todos los dispositivos que tienen, en su descripción, alguna de las palabras indicadas.

    **Ejemplo**:

    Para encontrar una frase que contenga las palabras **secundario** o **virtual**, puede incluir la expresión **secundario virtual** en la consulta.

    - **+**. Si agrega el signo + antes de una palabra, todos los resultados de búsqueda contendrán esa palabra.

    **Ejemplo**:

    Para encontrar una frase que contenga las palabras **secundario** y **virtual**, ingrese la consulta **+secundario+virtual**.

    - **-**. Si agrega el signo - antes de una palabra, ningún resultado de búsqueda contendrá esa palabra.

    **Ejemplo**:

    Para encontrar una frase que contenga **secundario** y no contenga **virtual**, ingrese la consulta **+secundario-virtual**.

    - **"<cadena>"**. El texto que se ingresa entre comillas debe estar presente en el texto.

    **Ejemplo**:

    Para encontrar una frase que contenga la combinación de palabras **servidor secundario**, puede ingresar **"servidor secundario"** en la consulta.

- Intervalo IP

  Si habilita esta opción, podrá ingresar las direcciones IP inicial y final del intervalo IP en el que deberán estar incluidos los dispositivos pertinentes.

  Esta opción está deshabilitada de forma predeterminada.

- Administrado por un Servidor de administración diferente

  Seleccione uno de los siguientes valores:

  - **Sí**. Una regla de movimiento de dispositivos solo se aplica a los dispositivos cliente administrados por otros Servidores de administración. Estos servidores son diferentes del servidor en el que configura la regla de movimiento de dispositivos.
  - **No**. La regla de movimiento de dispositivos solo se aplica a los dispositivos cliente administrados por el Servidor de administración actual.
  - **Ningún valor seleccionado**. La condición no se aplica.

En la sección **Controlador de dominio**, puede configurar criterios para incluir dispositivos en una selección según la suscripción de dominio:

- El dispositivo se encuentra en una unidad organizativa de dominio

  Si habilita esta opción, la selección incluirá los dispositivos de la unidad organizativa del dominio especificada en el campo de entrada.

  Esta opción está deshabilitada de forma predeterminada.

- El dispositivo es miembro del grupo de seguridad de dominio

  Si habilita esta opción, la selección incluirá los dispositivos que pertenezcan al grupo de seguridad de dominio especificado en el campo de entrada.

  Esta opción está deshabilitada de forma predeterminada.

En la sección **Actividad de red**, puede establecer los criterios que se usarán para incluir dispositivos en la selección basándose en la actividad de red de los mismos:

- Actúa como punto de distribución

  En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

  - **Sí**. La selección incluirá dispositivos que funcionen como punto de distribución.
  - **No**. La selección no incluirá dispositivos que funcionen como punto de distribución.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

- No desconectar del Servidor de administración

  En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

  - **Habilitado**. La selección incluirá dispositivos en los que esté activada la casilla **No desconectar del Servidor de administración**.
  - **Deshabilitado**. La selección incluirá dispositivos en los que no esté activada la casilla **No desconectar del Servidor de administración**.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

- Perfil de conexión cambiado

  En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

  - **Sí**. La selección incluirá dispositivos que se hayan conectado al Servidor de administración tras un cambio de perfil de conexión.
  - **No**. La selección no incluirá dispositivos que se hayan conectado al Servidor de administración tras un cambio de perfil de conexión.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

- Última conexión con el Servidor de administración

  Puede utilizar esta casilla para establecer un criterio de búsqueda de dispositivos que se base en el momento en el que haya ocurrido la última conexión al Servidor de administración.

  Si activa esta casilla, podrá usar los campos de entrada para indicar el intervalo de tiempo (fecha y hora) en el que deberá haber ocurrido la última conexión entre el Agente de red instalado en el dispositivo cliente y el Servidor de administración. La selección incluirá aquellos dispositivos que estén alcanzados por el intervalo especificado.

  Si no activa esta casilla, no se aplicará este criterio.

  Esta casilla no está marcada de manera predeterminada.

- Nuevos dispositivos detectados por sondeo de red

  Utilice esta opción para buscar dispositivos nuevos, que se hayan detectado durante los sondeos de red realizados en días recientes.

  Si habilita esta opción, la selección incluirá solo aquellos dispositivos nuevos que se hayan detectado mediante el descubrimiento de dispositivos en el intervalo de días especificado en el campo **Periodo de detección (días)**.

  Si deshabilita esta opción, la selección incluirá todos los dispositivos detectados por el mecanismo de descubrimiento.

  Esta opción está deshabilitada de forma predeterminada.

- Dispositivo visible

  En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

  - **Sí**. La selección incluirá aquellos dispositivos que sean visibles en la red.
  - **No**. La selección incluirá aquellos dispositivos que no sean visibles en la red.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

En la sección **Segmentos de nube**, puede configurar criterios para incluir dispositivos en una selección según sus respectivos segmentos de nube:

- El dispositivo se encuentra en un segmento de la nube

  Si esta opción está habilitada, puede elegir dispositivos de los segmentos de nube de AWS, Azure y Google.

  Si también habilita la opción **Incluir objetos secundarios**, la búsqueda se realizará en todos los objetos secundarios del segmento elegido.

  Los resultados de la búsqueda solo incluirán aquellos dispositivos que estén en el segmento seleccionado.

- Dispositivo encontrado mediante API

  La lista desplegable le permite operar con el hecho de que el dispositivo pueda detectarse con las herramientas provistas por una API.

  - **Sí**. El dispositivo se detecta mediante el uso de la API de AWS, Azure o Google.
  - **No**. El dispositivo no se puede detectar mediante el uso de la API de AWS, Azure o Google. Es decir, o bien el dispositivo no se encuentra en el entorno de nube, o bien sí está en el entorno de nube, pero, por algún motivo, no se lo puede detectar con una API.
  - Ningún valor. Esta condición no se aplica.

## Estados de los dispositivos

En la sección **Estado del dispositivo administrado**, puede configurar criterios para incluir dispositivos en una selección según la descripción del estado de dispositivos desde una aplicación administrada:

- **Estado del dispositivo**

  Lista desplegable en la que puede seleccionar un estado de dispositivo: *Sin inconvenientes*, *Crítico* o *Advertencia*.

- **Estado de protección en tiempo real**

  Lista desplegable en la cual puede seleccionar el estado de la protección en tiempo real. La selección incluirá aquellos dispositivos que tengan el estado de protección en tiempo real indicado.

- **Descripción del estado del dispositivo**

  En este campo, puede activar casillas correspondientes a condiciones que, al cumplirse, hacen que el dispositivo tome uno de los siguientes estados: *Sin inconvenientes, Crítico* o *Advertencia*.

En la sección **Estado de componentes en aplicaciones administradas**, puede configurar los criterios para incluir dispositivos en una selección según los estados de los componentes de las aplicaciones administradas:

- **Estado de Prevención de fugas de datos**

  Buscar dispositivos basándose en el estado de Prevención de fuga de datos (*Desconocido, Detenida, Iniciándose, En pausa, En ejecución, Error*).

- **Estado de protección de los servidores de colaboración**

  Buscar dispositivos basándose en el estado de la protección para servidores de colaboración (*Desconocido*, *Detenida*, *Iniciándose, En pausa*, *En ejecución*, *Error*).

- **Estado de protección antivirus en servidores de correo**

  Buscar dispositivos basándose en el estado de la protección para servidores de correo (*Desconocido, Detenida, Iniciándose, En pausa, En ejecución, Error).*

- **Estado de Sensor de Endpoint**

  Buscar dispositivos basándose en el estado del componente Sensor de Endpoint (*Desconocido, Detenida, Iniciándose, En pausa, En ejecución, Error*).

En la sección **Problemas que afectan al estado en las aplicaciones administradas**, puede especificar los criterios que se utilizarán para incluir dispositivos en la selección de acuerdo con la lista de posibles problemas detectados por una aplicación administrada. Si un dispositivo tiene al menos uno de los problemas elegidos, ese dispositivo se incluirá en la selección. Cuando selecciona un problema listado para varias aplicaciones, tiene la opción de seleccionar este problema en todas las listas automáticamente.

Puede activar casillas correspondientes a las descripciones de estado reportadas por la aplicación administrada. Cuando se reciban esos estados, los dispositivos correspondientes se incluirán en la selección. Si elige un estado incluido en las listas de varias aplicaciones, tendrá la opción de seleccionar todos los casos automáticamente.

## Datos del sistema

En la sección **Sistema operativo**, puede especificar los criterios que serán usados para incluir dispositivos en la selección según el tipo de sistema operativo.

- Tipo de plataforma

  Si activa esta casilla, podrá seleccionar un sistema operativo de la lista. Los dispositivos que tengan instalado ese sistema operativo se incluirán en los resultados de búsqueda.

- Versión del Service Pack del sistema operativo

  En este campo, puede especificar la versión del paquete de su sistema operativo (en formato *X.Y*), que determinará cómo aplicar la regla de migración a su dispositivo. De manera predeterminada, no hay una versión definida.

- Arquitectura del sistema operativo

  En la lista desplegable, puede seleccionar la arquitectura para la que deberá estar diseñado el sistema operativo. Los valores posibles son **Desconocido**, **x86**, **AMD64** e **IA64**. La arquitectura que elija determinará el modo de aplicar la regla de movimiento al dispositivo. De manera predeterminada, no hay ninguna opción seleccionada en la lista (es decir, la arquitectura del sistema operativo no está definida).

- Compilación del sistema operativo

  Este parámetro solo es válido para sistemas operativos Windows.

  Número de compilación del sistema operativo. Puede indicar si el número de compilación del sistema operativo seleccionado deberá ser igual, anterior o posterior al valor introducido. También puede hacer que la búsqueda incluya todos los números de compilación, excepto el especificado.

- Número de versión del sistema operativo

  Este parámetro solo es válido para sistemas operativos Windows.

  Identificador de versión del sistema operativo. Puede indicar si el sistema operativo seleccionado deberá tener un id. de versión igual, anterior o posterior al valor introducido. También puede hacer que la búsqueda incluya todos los id. de versión, excepto el especificado.

En la sección **Máquinas virtuales**, puede configurar los criterios que se usarán para incluir dispositivos en la selección basándose en el hecho de que sean máquinas virtuales o de que formen parte de una infraestructura de escritorios virtuales (VDI):

- Esta es una máquina virtual

  En la lista desplegable puede seleccionar las siguientes opciones:

  - **Sin definir**.
  - **No**. Buscar dispositivos que no sean máquinas virtuales.
  - **Sí**. Buscar dispositivos que sean máquinas virtuales.

- Tipo de máquina virtual

  En la lista desplegable, puede seleccionar el desarrollador de la máquina virtual.

  Esta lista desplegable estará disponible si seleccionó los valores **Sí** o **No es importante** en la lista desplegable **Es una máquina virtual**.

- Parte de la infraestructura de escritorio virtual

  En la lista desplegable puede seleccionar las siguientes opciones:

  - **Sin definir**.
  - **No**. Buscar dispositivos que no sean parte de la Infraestructura de escritorio virtual.
  - **Sí**. Buscar dispositivos que sean parte de una VDI.

En la sección **Registro de hardware**, puede configurar criterios para incluir dispositivos en una selección según el hardware que tengan instalado:

Asegúrese de que la utilidad lshw esté instalada en los dispositivos Linux desde los que desea obtener detalles del hardware. Los detalles de hardware obtenidos de las máquinas virtuales pueden estar incompletos según el hipervisor que se utilice.

- Dispositivo

  En la lista desplegable, puede seleccionar un tipo de unidad. Los dispositivos que tengan la unidad seleccionada se incluirán en los resultados de búsqueda.

  El campo permite realizar búsquedas de texto completo.

- Proveedor

  En la lista desplegable, puede seleccionar el nombre del fabricante de la unidad. Los dispositivos que tengan la unidad seleccionada se incluirán en los resultados de búsqueda.

  El campo permite realizar búsquedas de texto completo.

- **Nombre del dispositivo**

  Nombre del dispositivo en la red de Windows. El dispositivo con el nombre especificado se incluirá en la selección.

- **Descripción**

  Descripción del dispositivo o unidad de hardware. Los dispositivos que tengan la descripción indicada en este campo se incluirán en la selección.

  Si desea agregar una descripción a un dispositivo, puede hacerlo (en cualquier formato) a través de la ventana de propiedades del mismo. El campo permite realizar búsquedas de texto completo.

- **Proveedor del dispositivo**

  Nombre del fabricante del dispositivo. Los dispositivos producidos por el fabricante especificado en este campo se incluyen en la selección.

  Puede ingresar el nombre del fabricante en la ventana de propiedades de un dispositivo.

- **Número de serie**

  Todas las unidades de hardware con el número de serie especificado en este campo se incluirán en la selección.

- **Número de inventario**

  Los equipos que tengan el número de inventario indicado en este campo se incluirán en la selección.

- **Usuario**

  Todas las unidades de hardware del usuario especificado en este campo se incluirán en la selección.

- **Ubicación**

  Ubicación de un dispositivo o una unidad de hardware (por ejemplo, en la sede central o en una sucursal). Las computadoras o dispositivos que se encuentren en la ubicación especificada en este campo se incluirán en la selección.

  Puede describir la ubicación de un dispositivo en cualquier formato en la ventana de propiedades de dicho dispositivo.

- **Velocidad de reloj de la CPU, en MHz, desde**

  La frecuencia de reloj mínima de una CPU. Los equipos cuyas CPU coincidan con los intervalos especificados en estos campos de entrada (inclusive) se incluirán en la selección.

- Velocidad de reloj de la CPU, en MHz, hasta

  Intervalo de frecuencias de una CPU. Los equipos cuyas CPU coincidan con los intervalos especificados en estos campos de entrada (inclusive) se incluirán en la selección.

- Número de núcleos de CPU virtuales, desde

  El número mínimo de núcleos de CPU virtuales. Los equipos cuyas CPU coincidan con los intervalos de núcleos virtuales especificados en estos campos de entrada (inclusive) se incluirán en la selección.

- Número de núcleos de CPU virtuales, a

  El número máximo de núcleos de CPU virtuales. Los equipos cuyas CPU coincidan con los intervalos de núcleos virtuales especificados en estos campos de entrada (inclusive) se incluirán en la selección.

- Volumen del disco duro, en GB, desde

  El volumen mínimo del disco duro en el dispositivo. Los equipos cuyos discos duros coincidan con los intervalos especificados en estos campos de entrada (inclusive) se incluirán en la selección.

- Volumen de disco duro, en GB, hasta

  El volumen máximo del disco duro en el dispositivo. Los equipos cuyos discos duros coincidan con los intervalos especificados en estos campos de entrada (inclusive) se incluirán en la selección.

- Tamaño de RAM, en MB, desde

  El tamaño mínimo de la memoria RAM del dispositivo. Los dispositivos cuyas RAM coincidan con el intervalo de tamaño especificado en los campos de entrada (inclusive) se incluirán en la selección.

- Tamaño de RAM, en MB, hasta

  El tamaño máximo de la RAM de los dispositivos. Los dispositivos cuyas memorias RAM coincidan con los intervalos especificados en estos campos de entrada (inclusive) se incluirán en la selección.

## Detalles de software de terceros

En la sección **Registro de aplicaciones**, puede configurar los criterios para buscar dispositivos según aplicaciones instaladas en ellos:

- Nombre de la aplicación

  Lista desplegable en la que puede seleccionar una aplicación. Los dispositivos que tengan instalada la aplicación elegida se incluirán en la selección.

- Versión de la aplicación

  Campo de entrada en el que puede especificar la versión de la aplicación seleccionada.

- **Proveedor**

  Lista desplegable en la que puede seleccionar el desarrollador de una aplicación instalada en el dispositivo.

- **Estado de la aplicación**

  Lista desplegable en la que puede seleccionar el estado de la aplicación (*Instalada*, *Sin instalar*). Se incluirán en la selección los dispositivos que tengan o no tengan (dependiendo del estado seleccionado) la aplicación seleccionada.

- **Buscar por actualización**

  Si habilita esta opción, la búsqueda se basará en los detalles de las actualizaciones para el software instalado en los dispositivos pertinentes. Una vez que active esta casilla, los campos **Nombre de la aplicación**, **Versión de la aplicación** y **Estado de la aplicación** cambiarán a **Nombre de actualización**, **Versión de actualización** y **Estado**, respectivamente.

  Esta opción está deshabilitada de forma predeterminada.

- **Nombre de la aplicación de seguridad incompatible**

  Lista desplegable en la que puede seleccionar aplicaciones de seguridad de terceros. Los dispositivos que tengan instalada la aplicación seleccionada serán incluidos en la selección cuando se realice la búsqueda.

- **Etiqueta de aplicación**

  Lista desplegable en la que puede seleccionar una etiqueta de aplicación. Se incluirán en la selección aquellos dispositivos que tengan instaladas aplicaciones que, en su descripción, contengan la etiqueta seleccionada.

- **Aplicar a los dispositivos que no tengan las etiquetas especificadas**

  Si habilita esta opción, la selección incluirá aquellos dispositivos que no contengan ninguna de las etiquetas seleccionadas en su descripción.

  Si deshabilita esta opción, no se aplicará el criterio.

  Esta opción está deshabilitada de forma predeterminada.

En la sección **Vulnerabilidades y actualizaciones**, puede especificar los criterios que se usarán para incluir dispositivos en la selección basándose en el origen de Windows Update que utilicen:

**WUA está ahora conectado al Servidor de administración**

En la lista desplegable, puede seleccionar una de las siguientes opciones de búsqueda:

- **Sí**. Si selecciona esta opción, los resultados de búsqueda incluirán aquellos dispositivos que reciban sus actualizaciones de Windows Update del Servidor de administración.
- **No**. Si selecciona esta opción, los resultados incluirán aquellos dispositivos que reciban sus actualizaciones de Windows Update de cualquier otro origen.

## Detalles de las aplicaciones de Kaspersky

En la sección **Aplicaciones de Kaspersky**, puede configurar criterios para incluir dispositivos en una selección según la aplicación administrada seleccionada:

- Nombre de la aplicación

  En la lista desplegable, puede definir un criterio para incluir dispositivos en la selección cuando se realice una basada en el nombre de una aplicación de Kaspersky.

  La lista solo contendrá los nombres de aquellas aplicaciones que tengan su respectivo complemento de administración instalado en la estación de trabajo del administrador.

  Si no selecciona ninguna aplicación, este criterio no se aplicará.

- Versión de la aplicación

  En el campo de entrada, puede definir un criterio para incluir dispositivos en la selección cuando se realice una búsqueda basada en el número de versión de una aplicación de Kaspersky.

  Si no especifica un número de versión, este criterio no se aplicará.

- Nombre de la actualización crítica

  Lista desplegable en la que puede seleccionar el estado de la aplicación (*Instalada*, *Sin instalar*). Se incluirán en la selección los dispositivos que tengan o no tengan (dependiendo del estado seleccionado) la aplicación seleccionada.

  En el campo de entrada, puede definir un criterio para incluir dispositivos en la selección cuando se realice una búsqueda basada en el nombre de una aplicación o en un número de paquete de actualización.

  Si el campo queda en blanco, este criterio no se aplicará.

- Seleccione el período de la última actualización de módulos

  Use esta opción para definir un criterio que permita buscar dispositivos según la hora en que se hayan actualizado por última vez los módulos de las aplicaciones instaladas en ellos.

  Si activa esta casilla, podrá utilizar los campos de entrada para definir el intervalo de tiempo (fecha y hora) en el que deberá haber ocurrido la última actualización de módulos de las aplicaciones instaladas en los dispositivos.

  Si no activa esta casilla, no se aplicará este criterio.

  Esta casilla no está marcada de manera predeterminada.

- El dispositivo se administra a través del Servidor de administración

  Puede usar la lista desplegable para que la selección incluya aquellos dispositivos que se administren mediante Kaspersky Security Center:

  - **Sí**. La selección incluirá aquellos dispositivos que se administren mediante Kaspersky Security Center.
  - **No**. La aplicación incluirá aquellos dispositivos que no se administran mediante Kaspersky Security Center Linux.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

- La aplicación de seguridad está instalada

  Puede usar la lista desplegable para que la selección incluya aquellos dispositivos que tengan instalada la aplicación de seguridad:

  - **Sí**. La selección incluirá aquellos dispositivos en los que se haya instalado la aplicación de seguridad.
  - **No**. La selección incluirá aquellos dispositivos en los que no se haya instalado la aplicación de seguridad.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

En la sección **Protección antivirus**, puede configurar los criterios para incluir dispositivos en una selección en función de su estado de protección:

- Bases de datos publicadas

  Seleccione esta opción para buscar dispositivos cliente basándose en la fecha de publicación de las bases de datos antivirus. Utilice el campo de entrada para definir el intervalo de tiempo que se tomará como base para la búsqueda.

  Esta opción está deshabilitada de forma predeterminada.

- Registros de la base de datos

  Si se habilita esta opción, podrá buscar los dispositivos cliente por el número de registros de la base de datos. En los campos de entrada puede establecer los valores umbral más bajos y más altos de los registros de la base de datos antivirus.

  Esta opción está deshabilitada de forma predeterminada.

- **Último análisis**

  Habilite esta opción para buscar dispositivos cliente basándose en la hora del último análisis antimalware. Utilice los campos de entrada para definir el período en el cual deberá haber ocurrido el último análisis antimalware.

  Esta opción está deshabilitada de forma predeterminada.

- **Amenazas detectadas**

  Habilite esta opción para buscar dispositivos cliente basándose en el número de virus detectados. Utilice los campos de entrada para definir los valores que se tomarán como umbral superior e inferior del número de virus detectados.

  Esta opción está deshabilitada de forma predeterminada.

En la subsección **Cifrado**, puede configurar criterios para incluir dispositivos en una selección según el algoritmo de cifrado seleccionado:

**Algoritmo de cifrado**

Algoritmo de cifrado de bloque simétrico AES. En la lista desplegable, puede seleccionar el tamaño de la clave de cifrado (56 bits, 128 bits, 192 bits o 256 bits).

Valores disponibles: *AES56*, *AES128*, *AES192* y *AES256*.

La subsección **Componentes de las aplicaciones** contiene la lista de componentes de aquellas aplicaciones que tienen los complementos de administración correspondientes instalados en Kaspersky Security Center Cloud Console.

En la sección **Componentes de las aplicaciones**, puede definir criterios para incluir dispositivos en la selección basándose en los estados y los números de versión de los componentes vinculados a la aplicación seleccionada:

- **Estado**

  Buscar dispositivos basándose en el estado de un componente reportado por una aplicación al Servidor de administración. Puede seleccionar uno de los siguientes estados: *N/D, Detenido*, *En pausa*, *Iniciándose*, *En ejecución, Error, Sin instalar, No compatible con la licencia*. Si el componente seleccionado de la aplicación instalada en un dispositivo administrado tiene el estado especificado, el dispositivo será incluido en la selección de dispositivos.

  Estados reportados por las aplicaciones:

  - *Detenido*: el componente está deshabilitado y no se encuentra en funcionamiento.
  - *En pausa*: el componente se encuentra suspendido (por ejemplo, porque el usuario pausó la protección en la aplicación administrada).
  - *Iniciándose*: el componente está en proceso de iniciarse.
  - *En ejecución*: el componente está habilitado y funciona correctamente.
  - *Error*: ocurrió un error durante el funcionamiento del componente.
  - *Sin instalar*: el usuario no optó por instalar el componente al realizar una instalación personalizada de la aplicación.
  - *No compatible con la licencia*: la licencia no cubre el componente seleccionado.

  A diferencia de los demás estados, *N/D* no es un estado reportado por las aplicaciones. Se trata de una opción que muestra que las aplicaciones no tienen información sobre el estado del componente seleccionado. Esta situación puede presentarse, por ejemplo, cuando el componente seleccionado no pertenece a ninguna de las aplicaciones instaladas en el dispositivo o cuando el dispositivo está apagado.

- **Versión**

  Buscar dispositivos basándose en el número de versión del componente seleccionado en la lista. Puede escribir un número de versión, por ejemplo `3.4.1.0`, y luego especificar si el componente seleccionado debe tener una versión igual, anterior o posterior. También puede configurar la búsqueda de todas las versiones excepto la especificada.

## Etiquetas

En la sección **Etiquetas**, puede configurar criterios para dispositivos incluidos en una selección según palabras clave (etiquetas) que se agregaron anteriormente a las descripciones de dispositivos administrados:

**Aplicar si coincide al menos una etiqueta especificada**

Si habilita esta opción, los resultados de búsqueda mostrarán aquellos dispositivos que lleven, en su descripción, al menos una de las etiquetas seleccionadas.

Si deshabilita esta opción, los resultados de búsqueda solo mostrarán aquellos dispositivos que no tengan ninguna de las etiquetas seleccionadas en su descripción.

Esta opción está deshabilitada de forma predeterminada.

Para agregar etiquetas al criterio, haga clic en el botón **Agregar** y seleccione las etiquetas haciendo clic en el campo de entrada **Etiqueta**. Especifique si desea incluir o excluir los dispositivos con las etiquetas seleccionadas en la selección de dispositivos.

- **Todos los dispositivos que tengan esta etiqueta**

  Si selecciona esta opción, los resultados de búsqueda mostrarán aquellos dispositivos que lleven, en su descripción, la etiqueta seleccionada. La consulta de búsqueda puede incluir el asterisco, que representa una cadena de cualquier longitud (número de caracteres).

  Esta opción está seleccionada de manera predeterminada.

- **Todos los dispositivos que no tengan esta etiqueta**

  Si selecciona esta opción, los resultados de búsqueda mostrarán aquellos dispositivos que no lleven en su descripción la etiqueta seleccionada. La consulta de búsqueda puede incluir el asterisco, que representa una cadena de cualquier longitud (número de caracteres).

### Usuarios

En la sección **Usuarios**, puede configurar los criterios para incluir dispositivos en la selección basándose en las cuentas de usuario con las que se haya iniciado sesión en el sistema operativo.

- **Último usuario que inició sesión en el sistema**

  Si esta opción está habilitada, puede seleccionar la cuenta de usuario para configurar el criterio. Los resultados de búsqueda incluirán aquellos dispositivos en los que el usuario indicado haya sido el último en iniciar sesión.

- **Usuario que inició sesión en el sistema al menos una vez**

  Si habilita esta opción, podrá hacer clic en el botón **Examinar** para seleccionar una cuenta de usuario. Los resultados de búsqueda incluirán aquellos dispositivos en los que el usuario indicado haya iniciado sesión al menos una vez.

## Exportar la lista de dispositivos de una selección de dispositivos

Kaspersky Security Center le permite guardar información sobre dispositivos de una selección de dispositivos en un archivo CSV o TXT.

*Para exportar la lista de dispositivos de una selección de dispositivos, haga lo siguiente:*

1. Abra la tabla de dispositivos de la selección de dispositivos como se indica más arriba.
2. Utilice una de las siguientes formas para seleccionar los dispositivos que desea exportar:
   - Para seleccionar dispositivos específicos, seleccione las casillas de verificación junto a ellos.
   - Para seleccionar todos los dispositivos de la página de la tabla actual, seleccione la casilla de verificación en el encabezado de la tabla de dispositivos y luego seleccione la casilla de verificación **Seleccionar todo en la página actual**.
   - Para seleccionar todos los dispositivos de la tabla, seleccione la casilla de verificación en el encabezado de la tabla de dispositivos y luego seleccione la casilla de verificación **Seleccionar todo**.
3. Haga clic en el botón **Exportar a CSV** o **Exportar a TXT**. Se exportará toda la información sobre los dispositivos seleccionados incluidos en la tabla.

Tenga en cuenta que si aplicó un criterio de filtro a la tabla de dispositivos, solo se exportarán los datos filtrados de las columnas mostradas.

### Eliminación de dispositivos de los grupos de administración en una selección

Cuando se trabaja con la selección de dispositivos, puede eliminar los dispositivos de los grupos de administración en la misma selección, sin cambiar a los grupos de administración de los que se deben eliminar estos dispositivos.

*Para eliminar los dispositivos de los grupos de administración:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Selecciones de dispositivos** o a la sección **Descubrimiento y despliegue** → **Selecciones de dispositivos**.
2. En la lista de selecciones, haga clic en el nombre de la selección de dispositivos.

   La página muestra una tabla con información sobre los dispositivos incluidos en la selección de dispositivos.
3. Seleccione los dispositivos que desee eliminar y, a continuación, haga clic en **Eliminar**.

   Los dispositivos seleccionados se quitarán de los grupos de administración correspondientes.

## Etiquetas de dispositivo

Kaspersky Security Center le permite *etiquetar* dispositivos. Las etiquetas son rótulos que se asignan a los dispositivos y pueden usarse para agruparlos, describirlos o encontrarlos. Pueden utilizarse para crear selecciones, hallar dispositivos específicos y distribuir dispositivos en grupos de administración.

Puede etiquetar dispositivos manual o automáticamente. Si desea etiquetar un dispositivo específico, puede usar el etiquetado manual. Kaspersky Security Center realiza el etiquetado automático de una de las siguientes formas:

- Según las reglas de etiquetado especificadas.
- Mediante una aplicación.

No recomendamos que utilice diferentes formas de etiquetado para asignar la misma etiqueta. Por ejemplo, si la regla asigna una etiqueta, no se recomienda asignarla a los dispositivos manualmente.

Si las etiquetas se asignan mediante reglas, los dispositivos se etiquetan automáticamente cuando se cumplen las reglas especificadas. Cada regla está asociada a una sola etiqueta. Las reglas atienden a las propiedades de cada dispositivo, como sus atributos de red, su sistema operativo o las aplicaciones que tiene instaladas. Por ejemplo, si tiene una infraestructura híbrida de máquinas físicas, instancia de Amazon EC2 y máquinas virtuales de Microsoft Azure, puede configurar una regla que asignará la etiqueta `[Azure]` a todas las máquinas virtuales de Microsoft Azure. A continuación, puede usar esta etiqueta al crear una selección de dispositivos; esto le ayudará a clasificar todas las máquinas virtuales de Microsoft Azure y a asignarles una tarea.

Solo puede agregar una regla de etiquetado automático por etiqueta. Si crea una nueva regla para la misma etiqueta, se reemplazará la anterior.

Un dispositivo pierde una etiqueta en los siguientes casos:

- El dispositivo deja de reunir las condiciones indicadas en la regla que le asignó la etiqueta.
- Se elimina o se deshabilita la regla que le asignó al dispositivo la etiqueta.

Cada Servidor de administración tiene sus propias listas de reglas y de etiquetas, que son independientes de las listas de otros servidores de administración (esto incluye, si corresponde, el Servidor de administración principal o cualquier Servidor de administración virtual subordinado). Cada regla se aplica solo a los dispositivos del Servidor de administración en el que la regla se ha creado.

## Creación de una etiqueta de dispositivo

*Para crear una etiqueta de dispositivo:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Etiquetas** → **Etiquetas del dispositivo**.
2. Haga clic en **Agregar**.

   Se abre una ventana para crear la etiqueta.
3. En el campo **Etiqueta**, escriba el nombre de la etiqueta.
4. Haga clic en **Guardar** para guardar los cambios.

La nueva etiqueta aparece en la lista de etiquetas de dispositivo.

## Cambiar el nombre de una etiqueta de dispositivo

*Para cambiar el nombre de una etiqueta de dispositivo:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Etiquetas** → **Etiquetas del dispositivo**.
2. Haga clic en el nombre de la etiqueta que desee modificar.
   Se abre la ventana de propiedades de la etiqueta.
3. En el campo **Etiqueta**, cambie el nombre de etiqueta.
4. Haga clic en **Guardar** para guardar los cambios.

La etiqueta actualizada aparece en la lista de etiquetas de dispositivo.

## Eliminar una etiqueta de dispositivo

*Para eliminar una etiqueta de dispositivo:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Etiquetas** → **Etiquetas del dispositivo**.
2. En la lista, seleccione la etiqueta de dispositivo que desee eliminar.
3. Haga clic en el botón **Eliminar**.
4. En la ventana que se abre, haga clic en **Sí**.

Se elimina la etiqueta de dispositivo. La etiqueta eliminada se borra automáticamente de todos los dispositivos a los que estaba asignada.

La etiqueta eliminada no desaparecerá automáticamente de las reglas de etiquetado automático. Después de eliminar la etiqueta, se la asignará a un nuevo dispositivo solo cuando el dispositivo reúna las condiciones de una regla que asigne esa etiqueta.

El dispositivo no perderá automáticamente la etiqueta eliminada si la misma fue asignada por una aplicación o por el Agente de red. Para eliminar la etiqueta del dispositivo, use la utilidad klscflag.

## Ver los dispositivos que tienen asignada una etiqueta

*Para ver cuáles dispositivos tienen asignada una etiqueta:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Etiquetas** → **Etiquetas del dispositivo**.
2. Haga clic en el vínculo **Ver dispositivos** junto a una etiqueta para ver a qué dispositivos se la ha asignado.

   Se le redirigirá a la sección **Dispositivos administrados** del menú principal, donde verá los dispositivos filtrados según la etiqueta en la que haya hecho clic en el vínculo **Ver dispositivos**.
3. Para regresar a la lista de etiquetas de dispositivo, haga clic en el botón **Atrás** de su navegador.

Después de ver los dispositivos que tienen asignada la etiqueta, puede crear y asignar una nueva etiqueta o asignar la etiqueta existente a otros dispositivos. En este caso, debe eliminar el filtro por etiqueta, seleccionar los dispositivos y luego asignar la etiqueta.

## Ver las etiquetas asignadas a un dispositivo

*Para ver las etiquetas asignadas a un dispositivo:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.
2. Haga clic en el nombre del dispositivo cuyas etiquetas desee ver.
3. En la ventana que se abre, que contendrá las propiedades del dispositivo, elija la pestaña **Etiquetas**.

   Se muestra la lista de etiquetas asignadas al dispositivo seleccionado. En la columna **Modo de asignación**, puede ver cómo se asignó la etiqueta.

En la barra de herramientas, puede hacer lo siguiente:

- Asignar otra etiqueta al dispositivo.
- Eliminar una etiqueta ya asignada.
- Ver una lista con todas las etiquetas de dispositivo creadas en el Servidor de administración.

No puede ver las etiquetas asignadas localmente en el dispositivo.

## Etiquetar un dispositivo manualmente

*Para asignar una etiqueta a un dispositivo manualmente:*

1. Vea las etiquetas asignadas al dispositivo al que desee asignar otra etiqueta.
2. Haga clic en **Agregar**.

3. En la ventana que se abre, realice una de las siguientes acciones:

   - Para crear y asignar una nueva etiqueta, seleccione **Crear nueva etiqueta** y luego escriba el nombre de la nueva etiqueta.

   - Para seleccionar una etiqueta existente, seleccione **Asignar etiqueta existente** y luego, en la lista desplegable, elija la etiqueta pertinente.

4. Haga clic en **Aceptar** para aplicar los cambios.

5. Haga clic en **Guardar** para guardar los cambios.

La etiqueta seleccionada se asigna al dispositivo.

## Quitarle una etiqueta a un dispositivo

*Para quitarle una etiqueta a un dispositivo:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.

2. Haga clic en el nombre del dispositivo cuyas etiquetas desee ver.

3. En la ventana que se abre, que contendrá las propiedades del dispositivo, elija la pestaña **Etiquetas**.

4. Marque la casilla de verificación adyacente a la etiqueta que desee quitar del dispositivo.

5. Al principio de la lista, haga clic en el botón **¿Desea desasignar la etiqueta?**.

6. En la ventana que se abre, haga clic en **Sí**.

El dispositivo pierde la etiqueta.

La etiqueta desasignada no se elimina. Si lo desea, puede eliminarla manualmente.

Las etiquetas asignadas a un dispositivo por una aplicación o por el Agente de red no se pueden eliminar manualmente. Para eliminar estas etiquetas, utilice la utilidad klscflag.

## Ver las reglas de etiquetado automático de dispositivos

*Para ver las reglas que se utilizan para etiquetar dispositivos automáticamente,*

Realice una de las siguientes acciones:

- En el menú principal, vaya a **Activos (dispositivos)** → **Etiquetas** → **Reglas de etiquetado automático**.

- En el menú principal, vaya a **Activos (dispositivos)** → **Etiquetas** → **Etiquetas del dispositivo** y luego haga clic en el vínculo **Configurar reglas de etiquetado automático**.

- Vea las etiquetas asignadas a un dispositivo y después haga clic en el botón **Configuración**.

Se mostrará una lista con las reglas de etiquetado automático de dispositivos.

## Modificación de una regla para etiquetar dispositivos automáticamente

*Para modificar una regla para etiquetar dispositivos automáticamente:*

1. Vea las reglas de etiquetado automático de dispositivos.
2. Haga clic en el nombre de la regla que desee editar.

   Se abre una ventana para configurar la regla.
3. Modifique las propiedades generales de la regla:

   a. En el campo **Nombre de la regla**, cambie el nombre de regla.

   El nombre no puede contener más de 256 caracteres.

   b. Realice una de las siguientes acciones:

   - Pase el interruptor a **Regla habilitada** para habilitar la regla.
   - Pase el interruptor a **Regla deshabilitada** para deshabilitar la regla.
4. Realice una de las siguientes acciones:

   - Si desea agregar una condición, haga clic en el botón **Agregar** y, en la ventana que se abre, especifique la configuración de la nueva condición.
   - Si desea editar una condición existente, haga clic en el nombre de la condición que desee modificar y, a continuación, edite la configuración de la condición.
   - Si desea eliminar una condición, marque la casilla adyacente al nombre de la condición que desee eliminar y haga clic en **Eliminar**.
5. Haga clic en **Aceptar** en la ventana de configuración de condiciones.
6. Haga clic en **Guardar** para guardar los cambios.

La regla modificada se muestra en la lista.

## Creación de una regla para etiquetar dispositivos automáticamente

*Para crear una regla para etiquetar dispositivos automáticamente:*

1. Vea las reglas de etiquetado automático de dispositivos.
2. Haga clic en **Agregar**.

   Se abre una ventana para configurar la nueva regla.

3. Configure las propiedades generales de la regla:

   a. En el campo **Nombre de la regla**, escriba el nombre de la regla.

      El nombre no puede contener más de 256 caracteres.

   b. Realice una de las siguientes acciones:

      - Pase el interruptor a **Regla habilitada** para habilitar la regla.
      - Pase el interruptor a **Regla deshabilitada** para deshabilitar la regla.

   c. En el campo **Etiqueta**, escriba el nombre de una nueva etiqueta de dispositivo o seleccione una etiqueta de dispositivo de la lista.

      El nombre no puede contener más de 256 caracteres.

4. En la sección de condiciones, haga clic en el botón **Agregar** para añadir una nueva condición.

   Se abre una ventana para configurar la nueva condición.

5. Escriba el nombre de la condición.

   El nombre no puede contener más de 256 caracteres. No puede haber más de una condición con el mismo nombre dentro de una regla.

6. Configure las condiciones de activación de la regla. Puede seleccionar varias condiciones.

   - **Red**: atributos de red del dispositivo (por ejemplo, el nombre del dispositivo en la red de Windows o su pertenencia a un dominio o a una subred IP).

     Si la intercalación con diferenciación entre mayúsculas y minúsculas está configurada para la base de datos utilizada para Kaspersky Security Center, respete las mayúsculas y minúsculas cuando ingrese el nombre DNS de un dispositivo. De lo contrario, la regla de etiquetado automático no funcionará.

   - **Aplicaciones**: presencia del Agente de red en el dispositivo, tipo y versión de sistema operativo, arquitectura del sistema operativo.
   - **Máquinas virtuales**: el hecho de que el dispositivo corresponda a un tipo concreto de máquina virtual.
   - **Controlador de dominio**: presencia del dispositivo en una unidad organizativa de Active Directory y membresía del dispositivo en un grupo de Active Directory.
   - **Registro de aplicaciones**: presencia de aplicaciones de distintos proveedores en el dispositivo.

7. Haga clic en **Aceptar** para guardar los cambios.

   Si es necesario, puede especificar varias condiciones para una misma regla. En ese caso, la etiqueta se asignará a cualquier dispositivo que cumpla con al menos una condición.

8. Haga clic en **Guardar** para guardar los cambios.

La nueva regla se aplicará a los dispositivos administrados del Servidor de administración seleccionado. Si la configuración de un dispositivo cumple con las condiciones de la regla, ese dispositivo recibirá la etiqueta.

Tras la ejecución inicial, la regla se aplicará en los siguientes casos:

- automática y periódicamente, atendiendo a la carga del servidor.
- cada vez que se edite la regla.
- cada vez que la regla se aplique manualmente.
- cada vez que el Servidor de administración detecte un cambio en la configuración de un dispositivo que reúna las condiciones de la regla o en la configuración de un grupo que contenga dicho dispositivo.

Puede crear más de una regla de etiquetado. Si crea varias reglas de etiquetado y un dispositivo cumple simultáneamente con las condiciones de todas ellas, dicho dispositivo recibirá varias etiquetas. Puede ver la lista de todas las etiquetas asignadas a un dispositivo en las propiedades del mismo.

## Ejecución de reglas para etiquetar dispositivos automáticamente

Cuando se ejecuta una regla, la etiqueta definida en las propiedades de la misma se asigna a los dispositivos que reúnen las condiciones especificadas en las propiedades de esa misma regla. Solo es posible ejecutar reglas activas.

*Para ejecutar reglas de etiquetado automático de dispositivos:*

1. Vea las reglas de etiquetado automático de dispositivos.
2. Active las casillas de verificación ubicadas junto a las reglas activas que quiera ejecutar.
3. Haga clic en el botón **Ejecutar regla**.

Se ejecutan las reglas seleccionadas.

## Eliminación de una regla para etiquetar dispositivos automáticamente

*Para eliminar una regla de etiquetado automático de dispositivos:*

1. Vea las reglas de etiquetado automático de dispositivos.
2. Marque la casilla ubicada junto a la regla que desee eliminar.
3. Haga clic en **Eliminar**.
4. En la ventana que se abre, haga clic de nuevo en **Eliminar**.

Se elimina la regla seleccionada. La etiqueta especificada en las propiedades de la regla se desasigna de los dispositivos que la tenían asignada.

La etiqueta desasignada no se elimina. Si lo desea, puede eliminarla manualmente.

## Administrar las etiquetas de los dispositivos con la utilidad klscflag

Para asignar un conjunto de etiquetas a un dispositivo, debe ejecutar la utilidad klscflag en el dispositivo cliente al que desea asignar etiquetas.

La utilidad klscflag sobrescribe las etiquetas existentes asignadas al dispositivo. Esto significa que puede agregar o eliminar etiquetas especificando el conjunto de etiquetas deseado en el comando. La utilidad no tiene comandos separados para agregar o eliminar etiquetas individuales. En su lugar, modifica todo el conjunto de etiquetas.

> Al especificar nombres de etiquetas en comandos como klscflag, se recomienda utilizar un enfoque de mayúsculas y minúsculas uniforme, como por ejemplo todo en mayúsculas. El uso de mayúsculas puede ayudar a evitar posibles problemas con etiquetas que difieren solo en mayúsculas y minúsculas, según la configuración del DBMS.

*Para asignar etiquetas a su dispositivo mediante la utilidad klscflag:*

1. Ejecute el símbolo del sistema de Windows usando derechos de administrador y, a continuación, cambie su directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en la carpeta donde está instalado el Agente de red. La ruta de instalación predeterminada es <Disco>: \ Archivos de programa (x86) \ Kaspersky Lab \ NetworkAgent.

2. Introduzca uno de los siguientes comandos:

   - Para asignar un conjunto de etiquetas:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\" NOMBRE DE LA ETIQUETA 1 \",\" NOMBRE DE LA ETIQUETA 2 \",\" NOMBRE DE LA ETIQUETA 3 \"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     dónde `[\" NOMBRE DE LA ETIQUETA 1 \",\" NOMBRE DE LA ETIQUETA 2 \",\" NOMBRE DE LA ETIQUETA 3 \"]` es la lista de etiquetas que desea asignar a su dispositivo.

     Si deja los corchetes vacíos, se eliminarán todas las etiquetas del dispositivo:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

   - Para asignar una nueva etiqueta a un conjunto de etiquetas existente:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\" NUEVO NOMBRE DE ETIQUETA \",\" NOMBRE DE LA ETIQUETA 1 \",\" NOMBRE DE LA ETIQUETA 2 \",\" NOMBRE DE LA ETIQUETA 3 \"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     donde `NUEVO NOMBRE DE ETIQUETA` es el nombre de la etiqueta que desea asignar a su dispositivo y `NOMBRE DE ETIQUETA 1`, `NOMBRE DE ETIQUETA 2`, `NOMBRE DE ETIQUETA 3` son los nombres de las etiquetas ya asignadas al dispositivo.

   - Para eliminar una etiqueta específica sin eliminar otras etiquetas ya asignadas al dispositivo, ejecute el comando con el conjunto de etiquetas actualizado.

     Por ejemplo, si sus etiquetas actuales son `NOMBRE DE ETIQUETA 1`, `NOMBRE DE ETIQUETA 2`, `NOMBRE DE ETIQUETA 3` y desea eliminar `NOMBRE DE ETIQUETA 2`, ejecute el siguiente comando:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\" NOMBRE DE LA ETIQUETA 1 \",\" NOMBRE DE LA ETIQUETA 3 \"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

3. Reinicie el servicio del Agente de red.

   La utilidad klscflag asigna a su dispositivo las etiquetas especificadas.

4. Si quiere asegurarse de que la utilidad klscflag haya asignado correctamente las etiquetas especificadas, vea las etiquetas asignadas al dispositivo.

También puede asignar etiquetas de dispositivos manualmente.

# Directivas y perfiles de directivas

En Kaspersky Security Center Web Console, puede crear directivas para las aplicaciones de Kaspersky. En esta sección se explica qué son, cómo se crean y cómo se modifican las directivas y los perfiles de directivas.

## Acerca de las directivas y perfiles de directivas

Una *directiva* es un conjunto de valores de configuración que se aplican a una aplicación de Kaspersky en un grupo de administración y sus subgrupos. Puede instalar varias aplicaciones de Kaspersky en los dispositivos de un grupo de administración. Con Kaspersky Security Center, puede crear una única directiva para cada aplicación de Kaspersky disponible en un grupo de administración. Una directiva tiene uno de los siguientes estados (consulte la tabla a continuación):

Estado de la directiva

| Estado | Descripción |
|---|---|
| Activa | La directiva que se encuentra vigente en un dispositivo. Solo puede haber una directiva activa para cada aplicación de Kaspersky en cada grupo de administración. Los dispositivos aplican los valores configurados en la directiva activa a la aplicación de Kaspersky. |
| Inactiva | Una directiva que no se encuentra vigente en un dispositivo. |
| Fuera de la oficina | Una directiva "fuera de la oficina" entra en vigor (es decir, se activa) cuando el dispositivo sale de la red corporativa. |

Las directivas funcionan de acuerdo con las siguientes reglas:

- Es posible configurar más de una directiva, con distintos valores, para una misma aplicación.
- Solo puede haber una directiva activa para la aplicación actual.
- Puede activar una directiva inactiva para responder a un evento específico. Por ejemplo, puede aplicar ajustes de protección antivirus más estrictos durante un brote de virus.
- Una directiva puede tener directivas secundarias.

En general, puede usar las directivas como preparativos para situaciones de emergencia, como un ataque de virus. Si sufriera un ataque a través de unidades USB, por ejemplo, podría activar una directiva que bloqueara el acceso a ese tipo de unidades. Al hacerlo, la directiva que se encontrara activa hasta ese momento se desactivaría automáticamente.

Para poder hacer frente a distintas situaciones sin tener que mantener un grupo de directivas que difieran entre sí en unos pocos valores de configuración, puede usar perfiles de directivas.

Un *perfil de directiva* es un subconjunto de valores de configuración que se agrupan bajo un nombre y reemplazan los valores de configuración de una directiva. Un perfil de directiva afecta la constitución de los ajustes vigentes de un dispositivo administrado. Los *ajustes vigentes* de un dispositivo son aquellos que se encuentran en vigor en el mismo en un momento dado como resultado de aplicar la directiva, el perfil de directiva y la configuración local de una aplicación.

Los perfiles de directivas funcionan de acuerdo con las siguientes reglas:

- Un perfil de directiva entra en vigor cuando se cumple una condición de activación específica.
- Los perfiles de directivas contienen valores de configuración que difieren de los especificados en la directiva.
- La activación de un perfil de directiva modifica los ajustes vigentes del dispositivo administrado.
- Una directiva puede tener un máximo de 100 perfiles de directiva.

## Acerca del candado y el bloqueo de ajustes

Cada ajuste de configuración disponible en una directiva tiene un interruptor de bloqueo acompañado de un candado de ícono (). En la siguiente tabla, se muestran los estados que puede tener el interruptor de bloqueo.

Estados del interruptor de bloqueo

| Estado | Descripción |
| --- | --- |
| Sin definir | Cuando un ajuste tiene un candado abierto a su lado y el interruptor de bloqueo está desactivado, el valor de dicho ajuste no se especifica a través de la directiva. El usuario puede modificar el valor del ajuste mediante la interfaz de la aplicación administrada. Estos ajustes se consideran *desbloqueados*. |
| Imponer | Cuando un ajuste tiene un candado cerrado a su lado y el interruptor de bloqueo está activado, el valor definido para ese ajuste es el que se aplica en los dispositivos sujetos a la directiva. El usuario no puede modificar el valor del ajuste mediante la interfaz de la aplicación administrada. Estos ajustes se consideran *bloqueados*. |

Recomendamos encarecidamente que cierre los bloqueos para la configuración de la directiva que desea aplicar en los dispositivos administrados. La configuración de la directiva desbloqueada se puede reasignar mediante la configuración de la aplicación Kaspersky en un dispositivo administrado.

Puede utilizar el interruptor de bloqueo para lo siguiente:

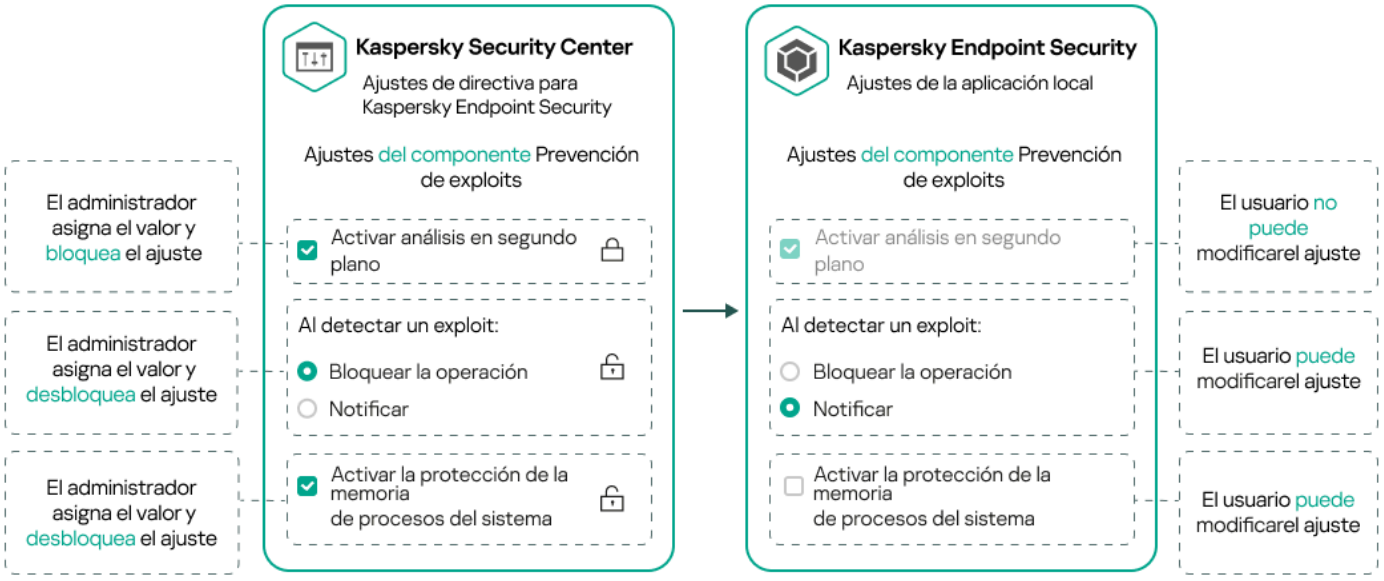
- Bloquear ajustes en la directiva de un subgrupo de administración
- Bloquear los ajustes de una aplicación de Kaspersky instalada en un dispositivo administrado

De este modo, un ajuste bloqueado se utiliza para formar y aplicar los ajustes vigentes de un dispositivo administrado.

El proceso para formar y aplicar los ajustes vigentes consta de las siguientes acciones:

- El dispositivo administrado aplica los valores de configuración definidos localmente en la aplicación de Kaspersky.
- El dispositivo administrado aplica los valores de configuración que se encuentran bloqueados en la directiva.

La directiva contiene los mismos ajustes que la aplicación de Kaspersky administrada. Cuando se modifican los ajustes dentro de una directiva, se modifican los ajustes en la aplicación de Kaspersky instalada en el dispositivo administrado. Los ajustes bloqueados no se pueden modificar en el dispositivo administrado (vea la siguiente imagen):




Candados y configuración de una aplicación de Kaspersky

# Herencia en las directivas y los perfiles de directivas

En esta sección, se brinda información sobre la jerarquía y la herencia en el ámbito de las directivas y los perfiles de directivas.

## Jerarquía de directivas

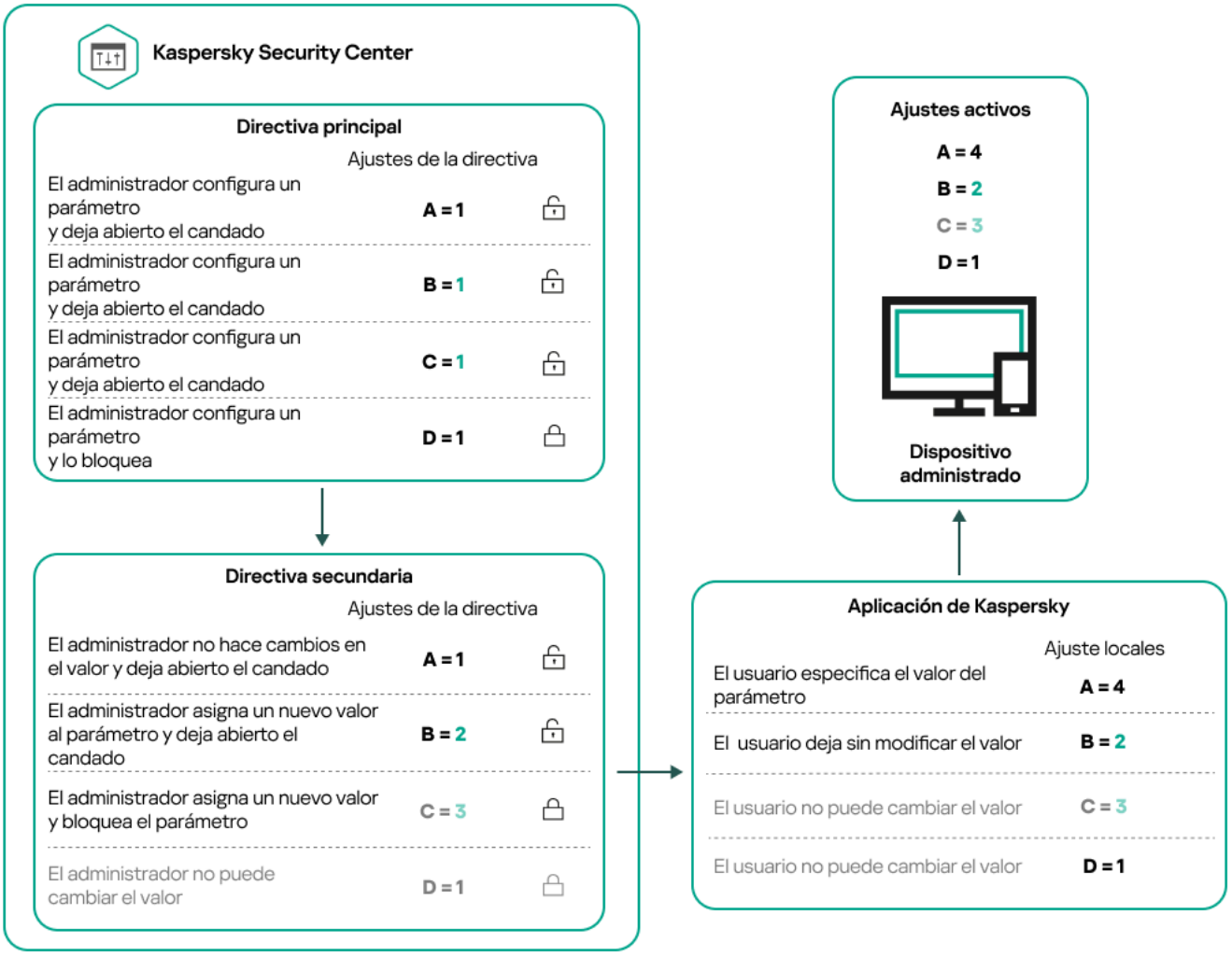
Si distintos dispositivos necesitan diferentes configuraciones, puede organizar los dispositivos en grupos de administración.

Puede especificar una directiva para un solo grupo de administración. La configuración de la directiva se puede *heredar*. La herencia hace que un subgrupo o grupo secundario de un grupo primario (un grupo de administración ubicado en un nivel superior) reciba valores de configuración de una directiva definida para ese grupo primario.

En lo sucesivo, se usará el término *directiva primaria* para hacer referencia a una directiva definida para un grupo primario. Una directiva para un subgrupo o grupo secundario se denominará *directiva secundaria*.

De forma predeterminada, existe al menos un grupo de dispositivos administrados en el Servidor de administración. Si crea grupos personalizados, se los creará como subgrupos o grupos secundarios de este grupo de dispositivos administrados.

Las directivas de una misma aplicación se afectan las unas a las otras siguiendo el orden jerárquico de los grupos de administración. Los ajustes que se bloquean en una directiva de un grupo de administración primario (de nivel superior) sobrescriben los valores de configuración en la directiva de un subgrupo (vea la siguiente imagen).

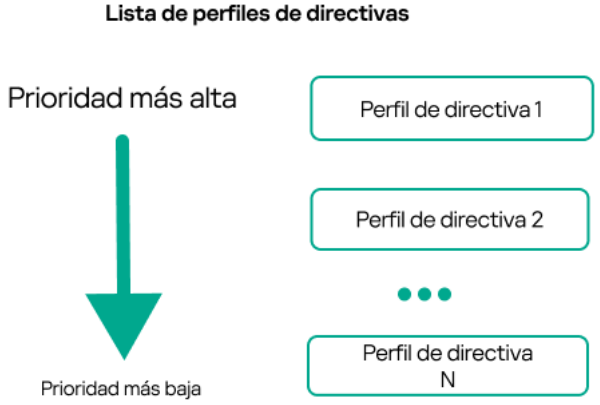



Jerarquía de directivas

## Perfiles de directivas en una jerarquía de directivas

Los perfiles de directivas tienen las siguientes condiciones de asignación de prioridad:

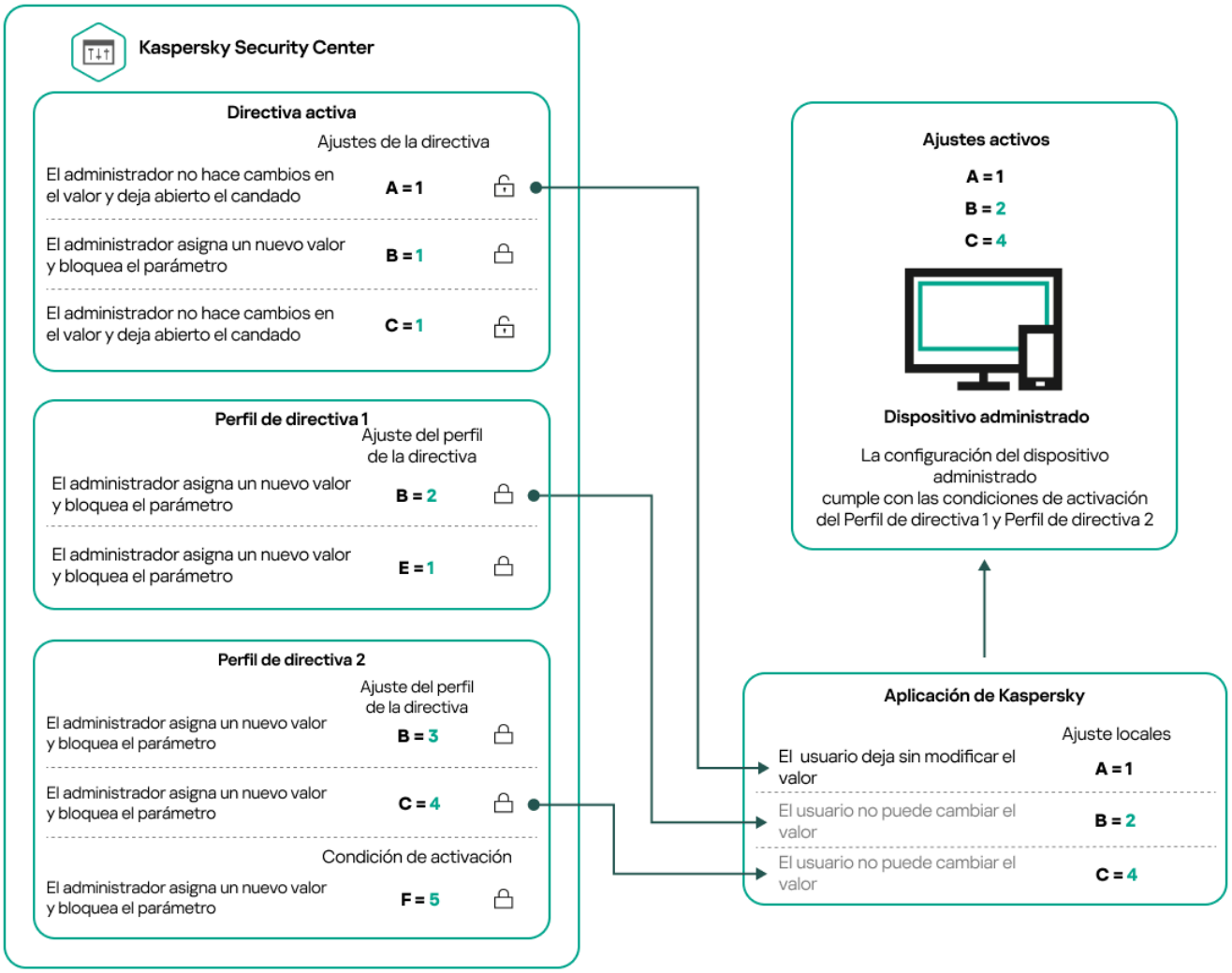
- La posición de un perfil en una lista de perfiles indica su prioridad. La prioridad de un perfil puede modificarse. La posición más alta en la lista representa la prioridad más alta (vea la siguiente imagen).




Definición de la prioridad de un perfil de directiva

- Las condiciones de activación de los perfiles de directivas no son interdependientes. Varios perfiles pueden activarse al mismo tiempo. Cuando un mismo ajuste de configuración se ve afectado por más de un perfil, el

dispositivo toma el valor de configuración indicado en el perfil de directiva de mayor prioridad (vea la siguiente imagen).

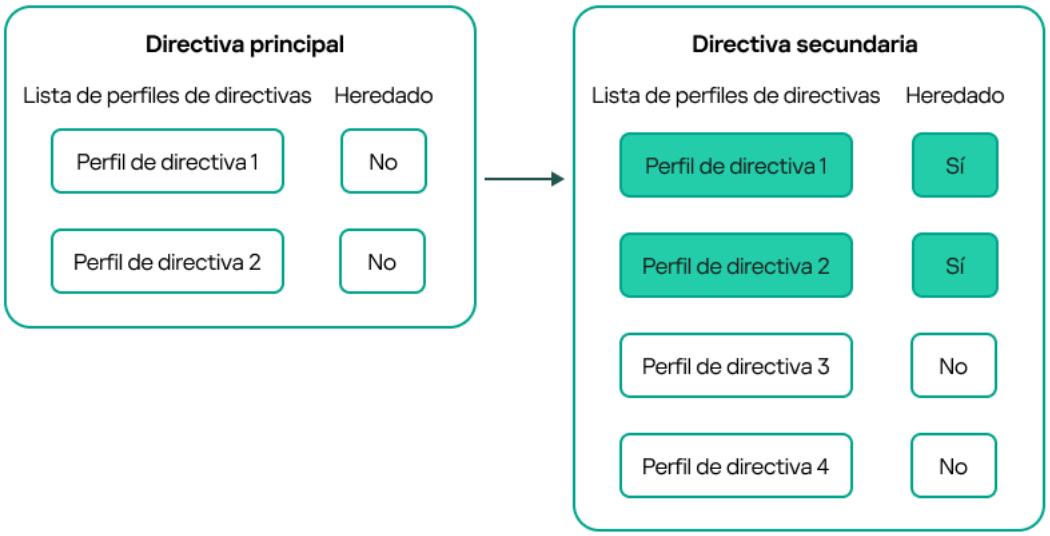



La configuración del dispositivo administrado cumple las condiciones de activación de varios perfiles de directiva

## Perfiles de directivas en una jerarquía de herencia

Los perfiles de directivas definidos para directivas de distintos niveles jerárquicos se rigen por estas condiciones:

- Una directiva de nivel inferior hereda los perfiles de una directiva de nivel superior. Un perfil de directiva que se ha heredado de una directiva de nivel superior obtiene mayor prioridad que el nivel del perfil de directiva original.
- No se puede cambiar la prioridad de un perfil de directiva heredado (vea la siguiente imagen).

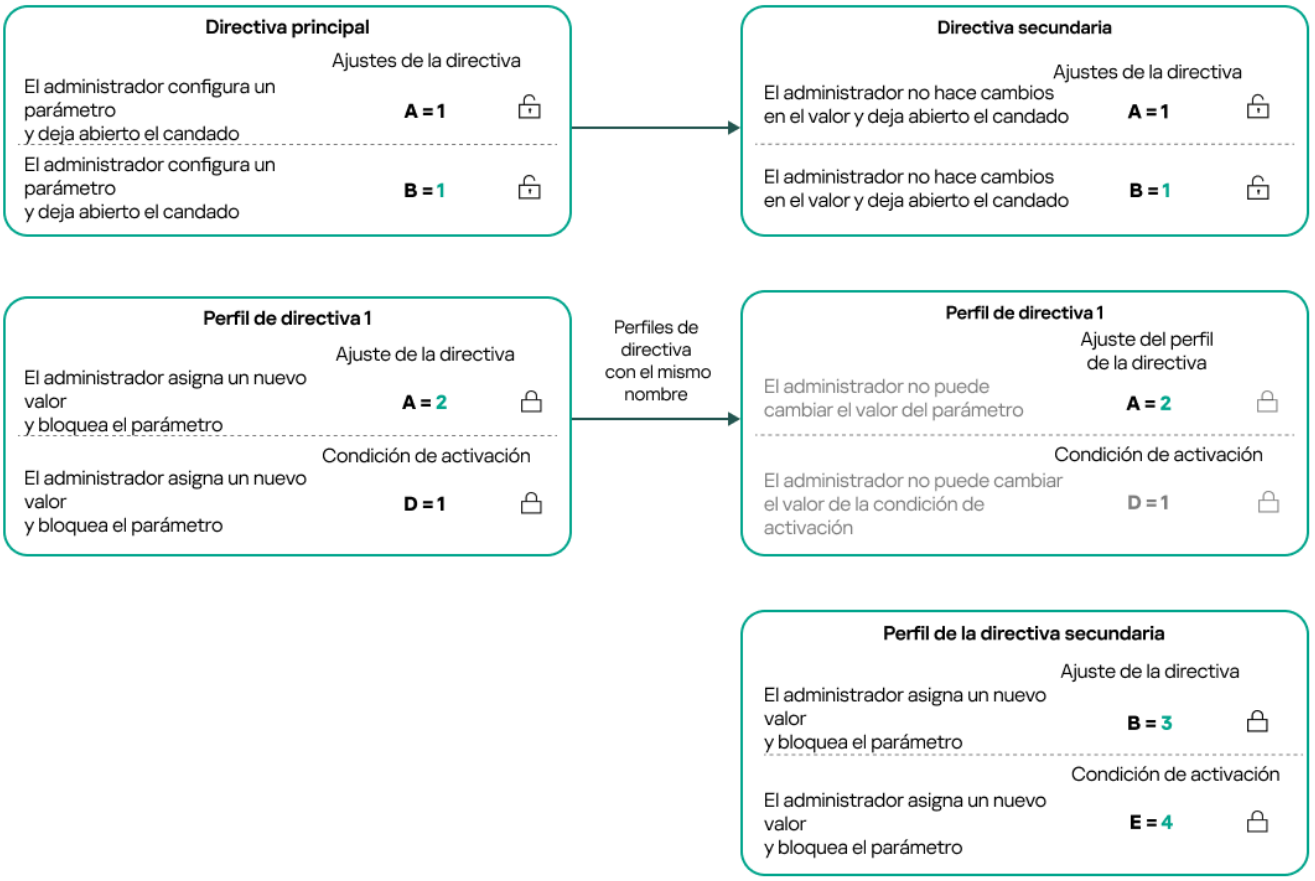



Herencia de perfiles de directivas

## Perfiles de directivas con el mismo nombre

Cuando existen dos directivas con el mismo nombre en niveles jerárquicos diferentes, esas directivas funcionan de acuerdo con las siguientes reglas:

- Los ajustes de configuración bloqueados y la condición de activación del perfil de directiva ubicado en el nivel superior cambian los ajustes y la condición de activación del perfil de directiva ubicado en el nivel inferior (vea la siguiente imagen).




El perfil secundario hereda los valores de configuración del perfil de directiva primario

- Los ajustes de configuración desbloqueados y la condición de activación del perfil de directiva ubicado en el nivel superior no cambian ni los ajustes ni la condición de activación del perfil de directiva ubicado en el nivel inferior.

## Cómo se implementan los valores de configuración en un dispositivo administrado

La implementación de los valores de configuración vigentes en un dispositivo administrado puede describirse de la siguiente manera:

- Todos los valores de configuración que no se bloquearon se toman de la directiva.
- Luego, estos valores se reemplazan con los valores configurados en la aplicación administrada.
- Finalmente, se aplican los valores de configuración que se encuentran bloqueados en la directiva en vigor. Los valores bloqueados sustituyen los valores de los ajustes vigentes que no estaban bloqueados.

# Administración de directivas

Esta sección trata sobre la administración de las directivas. Encontrará instrucciones para ver la lista de directivas; crear, copiar, modificar, mover o eliminar directivas; realizar una sincronización forzada, y ver un gráfico para conocer el estado de distribución de una directiva.

## Ver la lista de directivas

Puede ver listas con las directivas creadas para el Servidor de administración o para cualquier grupo de administración.

*Para ver una lista de directivas:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Jerarquía de grupos**.
2. En la estructura de grupos de administración, seleccione el grupo de administración al que corresponda la lista de directivas que desee ver.

   Aparece la lista de directivas en formato tabular. Si no hay ninguna directiva, la tabla estará vacía. Puede mostrar, ocultar y reorganizar las columnas de la tabla, utilizar la función de búsqueda o ver solo las líneas que contengan un valor especificado.

## Crear una directiva

Puede crear directivas nuevas y modificar o eliminar las directivas existentes.

*Para crear una directiva:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Seleccione el grupo de administración relacionado con la directiva:
   - Para el grupo root:

     En este caso, puede avanzar al próximo paso.
   - Para un subgrupo:

     a. Haga clic en el vínculo de la ruta actual en la parte superior de la ventana.

     b. En el panel que se abre, haga clic en el vínculo con el nombre del subgrupo requerido.

     La ruta actual cambia para reflejar el subgrupo seleccionado.
3. Haga clic en **Agregar**.

   Se abre la ventana **Seleccionar aplicación**.
4. Seleccione la aplicación para la que desee crear la directiva.

5. Haga clic en **Siguiente**.

   Se abre la ventana de configuración de la nueva directiva, con la pestaña **General** seleccionada.

6. Si lo desea, cambie el nombre predeterminado, el estado predeterminado y las opciones de directiva predeterminadas.

7. Seleccione la pestaña **Configuración de la aplicación**.

   O, si lo prefiere, haga clic en **Guardar** y salga de la ventana. La directiva se mostrará en la lista de directivas y podrá editar su configuración en otro momento.

8. En la pestaña **Configuración de la aplicación**, en el panel izquierdo, seleccione la categoría que desea y, en el panel de resultados de la derecha, edite la configuración de la directiva. Puede editar los ajustes de configuración disponibles en cada categoría (sección).

   El conjunto de configuraciones depende de la aplicación para el que crea una directiva. Para más detalles, consulte los siguientes recursos:

   - Configuración del Servidor de administración
   - Ajustes de la directiva del Agente de red
   - Documentación de Kaspersky Endpoint Security para Windows

   Para obtener detalles sobre la configuración de otras aplicaciones de seguridad, consulte la documentación de la aplicación correspondiente.

   Al editar la configuración, puede hacer clic en **Cancelar** para cancelar la última operación.

9. Haga clic en **Guardar** para guardar la directiva.

La directiva aparecerá en la lista de directivas.

## Modificar una directiva

*Para modificar una directiva:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en la directiva que desee modificar.

   Se abre la ventana de configuración de la directiva.

3. Especifique la configuración general y la configuración de la aplicación para la que crea una directiva. Para más detalles, consulte los siguientes recursos:

   - Configuración del Servidor de administración
   - Ajustes de la directiva del Agente de red
   - Documentación de Kaspersky Endpoint Security para Windows

   Si necesita información detallada para configurar otra aplicación de seguridad, consulte la documentación de ese software.

4. Haga clic en **Guardar**.

Los cambios realizados en la directiva se guardarán en las propiedades de la directiva y aparecerán en la sección **Historial de revisiones**.

## Ajustes generales de una directiva

### General

En la pestaña **General**, puede modificar el estado de la directiva y especificar la herencia de la configuración de la directiva:

- A través del bloque **Estado de la directiva**, puede seleccionar uno de los modos posibles para la directiva:
  - **Activa**

    Si se selecciona esta opción, se activa la directiva.

    Esta opción está seleccionada de forma predeterminada.

  - **Fuera de la oficina**

    Una directiva "fuera de la oficina" entra en vigor (es decir, se activa) cuando el dispositivo sale de la red corporativa.

  - **Inactiva**

    Si selecciona esta opción, la directiva estará inactiva, pero quedará guardada en la carpeta **Directivas**. Podrá activarla cuando resulte necesario.

- En el grupo de ajustes **Herencia de configuración**, puede configurar las opciones de directiva:
  - **Heredar configuración de la directiva primaria**

    Si habilita esta opción, la directiva heredará los valores de configuración definidos en la directiva del grupo de nivel superior. Estos valores, en consecuencia, estarán bloqueados.

    Esta opción está activada de forma predeterminada.

  - **Forzar la herencia de configuración en las directivas secundarias**

    Si habilita esta opción, cuando modifique la directiva y se apliquen los cambios, ocurrirá lo siguiente:
    - Los valores de configuración de la directiva se propagarán a las directivas de los subgrupos de administración (es decir, a las directivas secundarias).
    - En la ventana de propiedades de cada directiva secundaria, dentro del bloque **Herencia de configuración** de la sección **General**, se habilitará automáticamente la opción **Heredar configuración de la directiva primaria**.

    Habilitar esta opción hace que los ajustes de las directivas secundarias se bloqueen.

    Esta opción está deshabilitada de forma predeterminada.

## Configuración de eventos

La pestaña **Configuración de eventos** le permite configurar el registro de los eventos y las notificaciones de eventos. Los eventos están distribuidos por nivel de importancia en las siguientes pestañas:

- **Crítico**

  La sección **Crítico** no se muestra en las propiedades de la directiva del Agente de red.

- **Error funcional**
- **Advertencia**
- **Información**

Cada sección contiene una lista con los distintos tipos de eventos y la cantidad de días por las que cada evento se deja almacenado, de manera predeterminada, en el Servidor de administración. Haga clic en un tipo de evento para configurar los siguientes ajustes:

- **Registro de los eventos**

  Puede especificar cuántos días se conservará el evento y dónde se lo guardará:

  - **Exportar al sistema SIEM usando Syslog**
  - **Guardar en el registro de eventos del SO del dispositivo**
  - **Guardar en el registro de eventos del SO del Servidor de administración**

- **Notificaciones sobre los eventos**

  Puede seleccionar si desea ser notificado sobre el evento en uno de estos modos:

  - **Notificar por correo electrónico**
  - **Notificar por SMS**
  - **Notificar mediante la ejecución de un archivo ejecutable o un script**
  - **Notificar por SNMP**

  De forma predeterminada, se utilizan las opciones de notificación (por ejemplo, la dirección de destino) que se encuentran definidas en la pestaña de propiedades del Servidor de administración. Si desea modificar esta configuración, puede hacerlo a través de las pestañas **Correo electrónico**, **SMS** y **Archivo ejecutable para ejecutar**.

## Historial de revisiones

La pestaña **Historial de revisiones** le permite ver la lista de revisiones de la directiva y revertir los cambios realizados en la directiva, si es necesario.

## Habilitar y deshabilitar una opción de herencia en las directivas

*Para habilitar o deshabilitar la opción de herencia en una directiva:*

1. Abra la directiva que tenga en mente.
2. Abra la pestaña **General**.
3. Habilite o deshabilite la herencia en la directiva:
   - Si habilita la opción **Heredar configuración de la directiva primaria** en una directiva secundaria y un administrador bloquea algunos ajustes de configuración en la directiva primaria, no podrá cambiar esos ajustes en la directiva secundaria.
   - Si deshabilita la opción **Heredar configuración de la directiva primaria** en una directiva secundaria, podrá cambiar todos los ajustes de la directiva secundaria aunque haya ajustes bloqueados en la directiva primaria.
   - Si habilita la opción **Forzar la herencia de configuración en las directivas secundarias** en el grupo primario, se habilitará la opción **Heredar configuración de la directiva primaria** en cada directiva secundaria. No podrá deshabilitar esta opción en ninguna directiva secundaria. Los grupos secundarios heredarán por la fuerza todos los ajustes que se bloqueen en la directiva primaria; los valores de estos ajustes no se podrán modificar en los grupos secundarios.
4. Haga clic en el botón **Guardar** para guardar los cambios o haga clic en el botón **Cancelar** para rechazar los cambios.

De manera predeterminada, la opción **Heredar configuración de la directiva primaria** está habilitada en las directivas nuevas.

Si una directiva tiene perfiles, todas las directivas secundarias los heredan.

## Copiar una directiva

Puede copiar directivas de un grupo de administración a otro.

*Para copiar una directiva a otro grupo de administración:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Marque la casilla ubicada junto a la directiva (o las directivas) que desee copiar.
3. Haga clic en el botón **Copiar**.

   En el lado derecho de la pantalla, verá el árbol con los grupos de administración.
4. En el árbol, seleccione el grupo de destino (es decir, el grupo al que desee copiar la directiva o las directivas).
5. Haga clic en el botón **Copiar** que está al final de la pantalla.
6. Haga clic en **Aceptar** para confirmar la operación.

Las directivas que haya seleccionado se copiarán al grupo de destino con todos sus perfiles. El estado de estas directivas en el grupo de destino será **Inactiva**. Puede cambiar el estado a **Activa** en cualquier momento.

Si el grupo de destino contiene una directiva con el mismo nombre que la que se quiere mover, se agregará un índice secuencial —en formato (<siguiente número en la serie>), por ejemplo, (1)— al nombre de la directiva trasladada.

## Mover una directiva

Puede mover directivas de un grupo de administración a otro. Esto puede ser útil si necesita eliminar un grupo, por ejemplo, pero quiere utilizar sus directivas para un grupo diferente. En tal caso, antes de eliminar el grupo que ya no necesita, puede mover sus directivas al nuevo grupo.

*Para mover una directiva a otro grupo de administración:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Marque la casilla ubicada junto a la directiva (o las directivas) que desee mover.
3. Haga clic en el botón **Mover**.

   En el lado derecho de la pantalla, verá el árbol con los grupos de administración.
4. En el árbol, seleccione el grupo de destino (es decir, el grupo al que desee mover la directiva o las directivas).
5. Haga clic en el botón **Mover** en la parte inferior de la pantalla.
6. Haga clic en **Aceptar** para confirmar la operación.

   Si la directiva del grupo de origen no es una directiva heredada, se la moverá al grupo de destino junto con todos sus perfiles. El estado de la directiva en el grupo de destino será **Inactiva**. Puede cambiar el estado a **Activa** en cualquier momento.

   Si la directiva del grupo de origen es una directiva heredada, permanecerá en el grupo de origen. En lugar de moverla, se la copiará al grupo de destino junto con todos sus perfiles. El estado de la directiva en el grupo de destino será **Inactiva**. Puede cambiar el estado a **Activa** en cualquier momento.

Si el grupo de destino contiene una directiva con el mismo nombre que la que se quiere mover, se agregará un índice secuencial —en formato (<siguiente número en la serie>), por ejemplo, (1)— al nombre de la directiva trasladada.

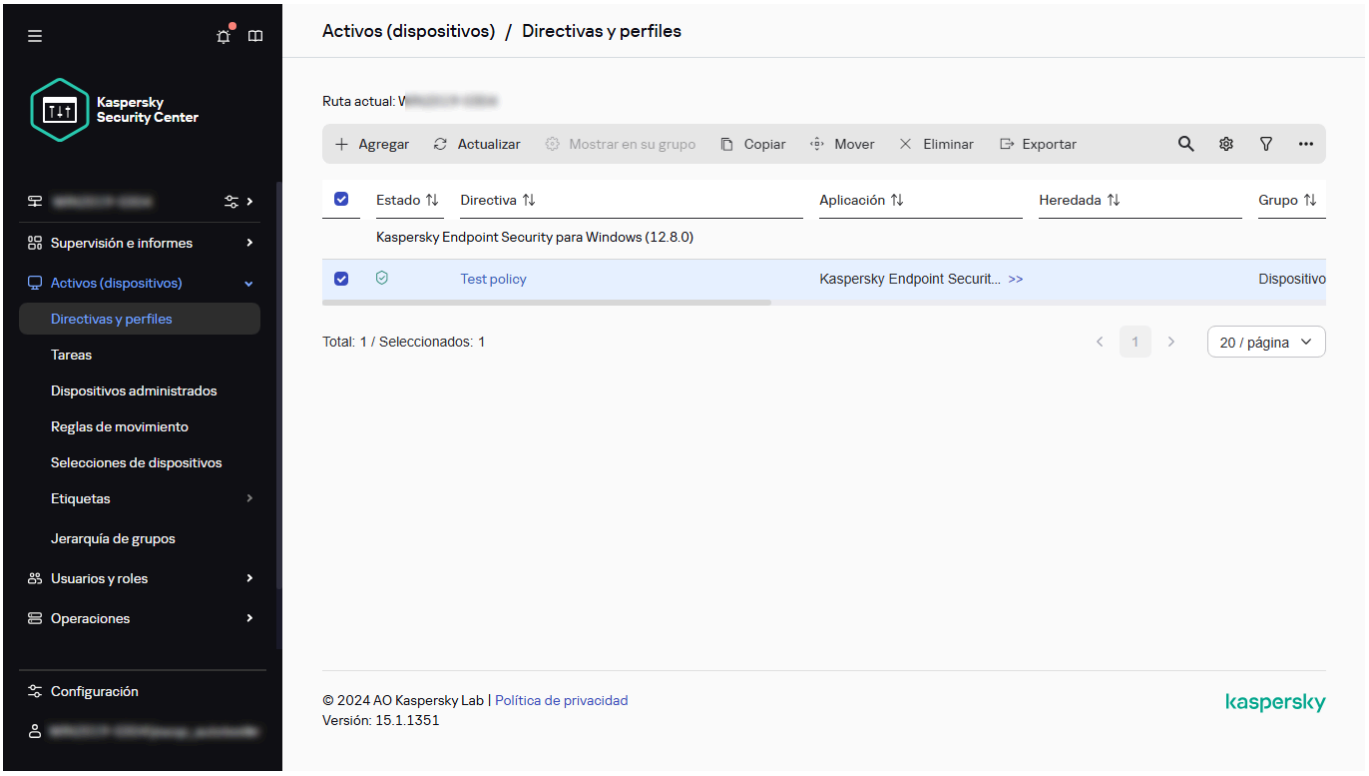
## Exportación de una directiva

Kaspersky Security Center permite guardar una directiva, su configuración y sus perfiles en un archivo KLP. El archivo KLP puede usarse para importar la directiva guardada en Kaspersky Security Center Windows o Kaspersky Security Center Linux.

*Para exportar una directiva:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Marque la casilla ubicada junto a la directiva que desee exportar.

   No es posible exportar más de una directiva a la vez. Si selecciona más de una directiva, el botón **Exportar** se desactivará.




3. Haga clic en el botón **Exportar**.
4. En la ventana **Guardar como** que se abrirá, ingrese la ruta y el nombre del archivo en el que se guardará la directiva. Haga clic en el botón **Guardar**.

   La ventana **Guardar como** aparecerá solo si utiliza los navegadores Google Chrome, Microsoft Edge u Opera. Si utiliza otro navegador, el archivo de la directiva se guardará automáticamente en la carpeta **Descargas**.

## Importación de una directiva

Kaspersky Security Center Linux permite importar una directiva guardada en un archivo KLP. El archivo KLP contiene la directiva exportada, su configuración y sus perfiles.

*Para importar una directiva:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el botón **Importar**.
3. Haga clic en el botón **Examinar** para elegir el archivo de política que desee importar.
4. En la ventana que se abrirá, ingrese la ruta al archivo KLP de la directiva y haga clic en el botón **Abrir**. Tenga en cuenta que no podrá seleccionar más de un archivo de directiva.

   Comenzará a procesarse la directiva.

5. Una vez que la directiva se haya procesado, seleccione el grupo de administración al que desee aplicarla.

6. Haga clic en el botón **Completado** para finalizar la importación de políticas.

Aparecerá una notificación con los resultados de la importación. Si la tarea se importa correctamente, puede hacer clic en el vínculo **Detalles** para ver las propiedades de la misma.

Una vez que se complete la importación, la directiva aparecerá en la lista de directivas. También se importarán la configuración y los perfiles de la directiva. La directiva importada tendrá estado inactivo independientemente del estado que se haya seleccionado al exportarla. Puede cambiar el estado en las propiedades de la directiva.

> Si la directiva importada tiene el mismo nombre que una directiva existente, el nombre de la directiva importada se complementará con un índice secuencial en formato **(<siguiente número secuencial>)**, por ejemplo **(1)** o **(2)**.

## Ver el gráfico de distribución de una directiva

Kaspersky Security Center cuenta con un gráfico de distribución de directivas que permite conocer el estado de aplicación de una directiva por dispositivo.

*Para ver el estado de distribución de una directiva en cada dispositivo:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.

2. Marque la casilla ubicada junto a la directiva cuyo estado de distribución desee conocer.

3. En el menú que aparece, seleccione el vínculo **Distribución**.

   Se abre la ventana **<Nombre de la directiva>: resultados de la distribución**.

4. En la ventana **<Nombre de la directiva>: resultados de la distribución**, encontrará la **Descripción del estado** de la directiva.

Puede cambiar la cantidad de resultados que aparecen en la lista que detalla la distribución de la directiva. El número máximo de dispositivos es 100 000.

*Para cambiar la cantidad de dispositivos que se muestran en la lista con los resultados de la distribución de una directiva:*

1. En el menú principal, vaya a la configuración de su cuenta y, a continuación, seleccione **Opciones de interfaz.**

2. En **Límite de dispositivos que se incluirán en los resultados de distribución de las directivas**, ingrese el número de dispositivos (hasta 100 000).

   De manera predeterminada, el límite es de 5000.

3. Haga clic en **Guardar**.

   El cambio se aplica y se guarda.

### Eliminar una directiva

Puede eliminar una directiva si ya no la necesita. Puede eliminar directivas que el grupo de administración especificado no haya heredado. Una directiva heredada solo se puede eliminar en el grupo de administración de nivel superior para el que fue creada.

*Para eliminar una directiva:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Marque la casilla ubicada junto a la directiva que desee eliminar y haga clic en **Eliminar**.

   El botón **Eliminar** no estará disponible (estará atenuado) si se ha seleccionado una directiva heredada.
3. Haga clic en **Aceptar** para confirmar la operación.

La directiva se elimina junto con todos sus perfiles.

## Administración de perfiles de directivas

Esta sección trata sobre la administración de perfiles de directivas. Encontrará instrucciones para ver los perfiles de una directiva; cambiar la prioridad de un perfil de directiva; crear, copiar, modificar o eliminar un perfil de directiva, y crear una regla de activación para un perfil de directiva.

### Ver los perfiles de una directiva

*Para ver los perfiles de una directiva:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva cuyos perfiles desee ver.

   Se abre la ventana de propiedades de la directiva, con la pestaña **General** seleccionada.
3. Abra la pestaña **Perfiles de directiva**.

Aparece la lista de perfiles de directiva en formato tabular. Si la directiva no tiene perfiles, verá una tabla vacía.

### Cambiar la prioridad de un perfil de directiva

*Para cambiar la prioridad de un perfil de directiva:*

1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva.
2. En la pestaña **Perfiles de directiva**, marque la casilla correspondiente al perfil de directiva que cambiará de prioridad.

3. Cambie la posición del perfil de directiva en la lista haciendo clic en los botones **Priorizar** o **Desprioritzar**.

   Cuanto más arriba en la lista se encuentre el perfil de directiva, mayor será su prioridad.

4. Haga clic en el botón **Guardar**.

Se aplica la nueva prioridad del perfil de directiva seleccionado.

## Crear un perfil de directiva

*Para crear un perfil de directiva:*

1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva. Si la directiva no tiene perfiles, verá una tabla vacía.

2. Haga clic en **Agregar**.

3. Si lo desea, cambie el nombre predeterminado y las opciones de directiva predeterminadas del perfil.

4. Seleccione la pestaña **Configuración de la aplicación**.

   O, si lo prefiere, puede hacer clic en **Guardar** y salir. El perfil que creó aparece en la lista de perfiles de directivas y podrá editar su configuración más adelante.

5. En la pestaña **Configuración de la aplicación**, en el panel izquierdo, seleccione la categoría que desea y, en el panel de resultados de la derecha, edite la configuración del perfil. Puede editar los ajustes disponibles en cada categoría (sección) para el perfil de directiva.

   Al editar la configuración, puede hacer clic en **Cancelar** para cancelar la última operación.

6. Haga clic en **Guardar** para guardar el perfil.

El perfil aparecerá en la lista de perfiles de directiva.

## Modificar un perfil de directiva

La posibilidad de modificar un perfil de directiva solo está disponible para las directivas de Kaspersky Endpoint Security para Windows.

*Para modificar un perfil de directiva:*

1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva.

2. En la pestaña **Perfiles de directiva**, seleccione el perfil de directiva que desee modificar.

   Se abre la ventana de propiedades del perfil de directiva.

3. En la ventana de propiedades, configure el perfil:

   - De ser necesario, en la pestaña **General**, habilite o deshabilite el perfil y cámbiele el nombre.
   - Modifique las reglas de activación del perfil.
   - Modifique los ajustes de la aplicación.

   Para obtener detalles sobre los ajustes de las aplicaciones de seguridad, consulte la documentación de esas aplicaciones.

4. Haga clic en **Guardar**.

Los cambios de configuración entrarán en vigor cuando el dispositivo se sincronice con el Servidor de administración (si el perfil de directiva está activo) o cuando se accione una de las reglas de activación (si el perfil de directiva está inactivo).

## Copiar un perfil de directiva

Puede copiar un perfil de directiva a la directiva actual o a otra si, por ejemplo, quiere tener perfiles idénticos para directivas diferentes. También puede copiar un perfil si necesita tener dos o más perfiles que se diferencien solo en un pequeño número de ajustes.

*Para copiar un perfil de directiva:*

1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva. Si la directiva no tiene perfiles, verá una tabla vacía.

2. En la pestaña **Perfiles de directiva**, seleccione el perfil de directiva que desee copiar.
3. Haga clic en **Copiar**.
4. En la ventana que se abre, seleccione la directiva a la que desee copiar el perfil.

   Puede copiar un perfil de directiva en la misma directiva o en una directiva que especifique.

5. Haga clic en **Copiar**.

   El perfil de directiva se copia a la directiva seleccionada. La copia del perfil obtiene la prioridad más baja. Cuando un perfil se copia a su misma directiva de origen, se agrega un índice numérico entre paréntesis al nombre de la copia (por ejemplo: (1), (2), etc.).

Más adelante, podrá cambiar la configuración del perfil, incluyendo su nombre y su prioridad; el perfil de directiva original no sufrirá modificaciones.

## Crear una regla de activación para un perfil de directiva

*Para crear una regla de activación para un perfil de directiva:*

1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva.

2. En la pestaña **Perfiles de directiva**, haga clic en el perfil de directiva para el que desee crear la regla de activación.

   Si la lista de perfiles de la directiva está vacía, puede crear un perfil de directiva.

3. En la pestaña **Reglas de activación**, haga clic en el botón **Agregar**.

   Se abre la ventana con las reglas de activación del perfil de directiva.

4. Escriba un nombre para la regla.

5. Active las casillas de verificación ubicadas junto a las condiciones que afectarán la activación del nuevo perfil de directiva:

- **Reglas generales para la activación del perfil de directiva**

  Marque esta casilla para configurar reglas que hagan que el perfil de directiva se active en un dispositivo dependiendo del estado del modo sin conexión de ese dispositivo, de las reglas de conexión con el Servidor de administración o de las etiquetas que el dispositivo tenga asignadas.

  Si elige esta opción, defina esto en el paso siguiente:

  - **Estado del dispositivo**

    Define la condición relativa a la presencia del dispositivo en la red:

    - **En línea**: el dispositivo está en la red, lo que significa que el Servidor de administración está disponible.
    - **Sin conexión**: el dispositivo está en una red externa, lo que significa que el Servidor de administración no está disponible.
    - **N/D**: no se aplica este criterio.

  - **Una regla de conexión al Servidor de administración está activa en este dispositivo**

    Elija la condición de activación del perfil de directiva (el hecho de que la regla se ejecute o no) y seleccione el nombre de la regla.

    La regla define la ubicación de red del dispositivo para la conexión con el Servidor de administración. Las condiciones de esta regla se deben cumplir (o no se deben cumplir) para que se active el perfil de directiva.

    Puede crear o configurar una descripción de ubicación de red de dispositivos para la conexión con un Servidor de administración en una regla de cambio de Agente de red.

- **Reglas para un propietario del dispositivo específico**

  Si elige esta opción, defina esto en el paso siguiente:

  - **Propietario del dispositivo**

    Habilite esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo dependiendo de quién sea el propietario del mismo. En la lista desplegable bajo la casilla, seleccione el criterio que determinará la activación del perfil:

    - El dispositivo pertenece al propietario especificado (signo "=").
    - El dispositivo no pertenece al propietario especificado (signo "#").

      Si habilita esta opción, el perfil se activará en el dispositivo siguiendo el criterio configurado. Podrá señalar al propietario del dispositivo una vez que habilite la opción. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

  - **El propietario del dispositivo está incluido en un grupo de seguridad interno**

Habilite esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo dependiendo de si su propietario pertenece a un grupo de seguridad interno de Kaspersky Security Center. En la lista desplegable bajo la casilla, seleccione el criterio que determinará la activación del perfil:

- El propietario del dispositivo es miembro del grupo de seguridad especificado (signo "=").
- El propietario del dispositivo no es miembro del grupo de seguridad especificado (signo "#").

  Si habilita esta opción, el perfil se activará en el dispositivo siguiendo el criterio configurado. Podrá especificar el nombre de un grupo de seguridad de Kaspersky Security Center. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

- Reglas para las especificaciones del hardware

  Marque esta casilla para configurar reglas que hagan que el perfil de directiva se active en un dispositivo dependiendo de la cantidad de memoria y del número de procesadores lógicos que el dispositivo tenga.

  Si elige esta opción, defina esto en el paso siguiente:

  - Tamaño de RAM, en MB

    Habilite esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo en función de la cantidad de RAM que este posea. En la lista desplegable bajo la casilla, seleccione el criterio que determinará la activación del perfil:
    - El tamaño de la RAM del dispositivo está por debajo del valor especificado (signo "<").
    - El tamaño de la RAM del dispositivo está por encima del valor especificado (signo ">").

    Si habilita esta opción, el perfil se activará en el dispositivo siguiendo el criterio configurado. Podrá especificar la cantidad de RAM con la que deberá contar el dispositivo. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

  - Número de procesadores lógicos

    Habilite esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo en función del número de procesadores lógicos que este tenga. En la lista desplegable bajo la casilla, seleccione el criterio que determinará la activación del perfil:
    - El número de procesadores lógicos del dispositivo es menor o igual que el valor especificado (signo "<").
    - El número de procesadores lógicos del dispositivo es mayor o igual que el valor especificado (signo ">").

    Si habilita esta opción, el perfil se activará en el dispositivo siguiendo el criterio configurado. Podrá especificar la cantidad de procesadores lógicos con los que deberá contar el dispositivo. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

- **Reglas para la asignación de roles**

  Si elige esta opción, defina esto en el paso siguiente:

Activar el perfil de directiva según el rol específico del propietario del dispositivo

Habilite esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo dependiendo del rol asignado al propietario del mismo. Utilice la lista de roles existentes para agregar el rol en forma manual.

Si habilita esta opción, el perfil se activará en el dispositivo siguiendo el criterio configurado.

- Reglas para el uso de la etiqueta

  Marque esta casilla para configurar reglas que hagan que el perfil de directiva se active en un dispositivo dependiendo de las etiquetas asignadas al mismo. El perfil de directiva podrá activarse en dispositivos que tengan las etiquetas seleccionadas o que no tengan esas etiquetas.

  Si elige esta opción, defina esto en el paso siguiente:

  - Etiqueta

    En la lista de etiquetas, configure la regla que hará que los dispositivos que tengan ciertas etiquetas se incluyan en el perfil de directiva. Para configurar esta regla, active las casillas ubicadas junto a las etiquetas pertinentes.

    Si necesita agregar etiquetas nuevas, introdúzcalas en el campo que se encuentra sobre la lista y haga clic en el botón **Agregar**.

    El perfil de directiva incluirá aquellos dispositivos que, en su descripción, contengan todas las etiquetas seleccionadas. Si no activa estas casillas, no se aplicará este criterio. Estas casillas están desactivadas de manera predeterminada.

  - Aplicar a los dispositivos que no tengan las etiquetas especificadas

    Habilite esta opción si tiene que invertir la selección de etiquetas.

    Si habilita esta opción, el perfil de directiva incluirá aquellos dispositivos que no tengan, en su descripción, ninguna de las etiquetas seleccionadas. Si deshabilita esta opción, no se aplicará el criterio.

    Esta opción está deshabilitada de forma predeterminada.

- Reglas para el uso de Active Directory

  Marque esta casilla para configurar reglas que hagan que el perfil de directiva se active en un dispositivo si el mismo pertenece a una unidad organizativa de Active Directory en particular o si el dispositivo o su propietario son miembros de un grupo de seguridad de Active Directory.

  Si elige esta opción, defina esto en el paso siguiente:

  - Membrecía del propietario del dispositivo en un grupo de seguridad de Active Directory

    Si habilita esta opción, el perfil de directiva se activará en un dispositivo si su propietario es miembro del grupo de seguridad especificado. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

  - Membrecía del dispositivo en un grupo de seguridad de Active Directory

Si habilita esta opción, el perfil de directiva se activará en el dispositivo. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

- **Asignación de dispositivos en la unidad organizativa de Active Directory**

  Si habilita esta opción, el perfil de directiva se activará en un dispositivo si el mismo está incluido en la unidad organizativa de Active Directory especificada. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil.

  Esta opción está deshabilitada de forma predeterminada.

El número de páginas adicionales del asistente dependerá de las opciones que haya elegido en el primer paso. Podrá modificar las reglas de activación del perfil de directiva más adelante.

6. Revise la lista de parámetros configurados. Si no hay errores en la lista, haga clic en **Crear**.

Se guardará el perfil. El perfil se activará en el dispositivo cuando se desencadenen las reglas de activación.

Las reglas de activación creadas para un perfil de directiva se muestran en las propiedades del perfil, dentro de la pestaña **Reglas de activación**. Puede modificar o eliminar cualquiera de las reglas de activación del perfil de directiva.

Existe la posibilidad de que varias reglas de activación se desencadenen simultáneamente.

### Eliminar un perfil de directiva

*Para eliminar un perfil de directiva:*

1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva.

2. En la pestaña **Perfiles de directiva**, marque la casilla ubicada junto al perfil de directiva que desee eliminar y haga clic en **Eliminar**.

3. En la ventana que se abre, haga clic de nuevo en **Eliminar**.

El perfil de directiva se elimina. Si la directiva es heredada por un grupo de nivel inferior, el perfil permanece en ese grupo pero se convierte en el perfil de la directiva de ese grupo. De este modo, se evitan cambios radicales en la configuración de las aplicaciones administradas que se encuentran instaladas en los dispositivos de los grupos de nivel inferior.

## Protección y cifrado de datos

El cifrado de datos reduce el riesgo de pérdida involuntaria de datos en caso de que le roben o pierda su computadora portátil o su disco duro, o en caso de que usuarios no autorizados y aplicaciones accedan a ellos.

Las siguientes aplicaciones de Kaspersky son compatibles con el cifrado de datos:

- Kaspersky Endpoint Security para Windows
- Kaspersky Endpoint Security for Mac

Puede modificar los ajustes de la interfaz de usuario para mostrar u ocultar algunos de los elementos de la interfaz que están vinculados a la función de administración del cifrado.

No recomendamos habilitar el cifrado en VDI.

### Cifrado de datos en Kaspersky Endpoint Security para Windows

Puede administrar los siguientes tipos de cifrado:

- Cifrado de unidad BitLocker, en dispositivos que tengan un sistema operativo Windows para servidores
- Cifrado de discos de Kaspersky en dispositivos que ejecutan un sistema operativo Windows para estaciones de trabajo

Al usar estos componentes de Kaspersky Endpoint Security para Windows puede, por ejemplo, activar o desactivar el cifrado, ver la lista de unidades cifradas o generar y ver informes sobre el cifrado.

Para configurar los ajustes de cifrado, deberá definir directivas de Kaspersky Endpoint Security para Windows a través de Kaspersky Security Center. Kaspersky Endpoint Security para Windows realizará las operaciones de cifrado y descifrado que se indiquen en la directiva activa. Si desea obtener instrucciones detalladas sobre cómo configurar reglas, así como una descripción de las funciones de cifrado, consulte la Ayuda de Kaspersky Endpoint Security para Windows.

### Cifrado de datos en Kaspersky Endpoint Security para Mac

En dispositivos con macOS, puede utilizar el cifrado FileVault. Esta tecnología de cifrado puede habilitarse y deshabilitarse a través de Kaspersky Endpoint Security for Mac.

Para configurar los ajustes de cifrado, deberá definir directivas de Kaspersky Endpoint Security for Mac a través de Kaspersky Security Center. Kaspersky Endpoint Security for Mac realizará las operaciones de cifrado y descifrado que se indiquen la directiva activa. Para obtener información detallada sobre las funciones de cifrado, consulte la Ayuda de Kaspersky Endpoint Security for Mac.

## Ver la lista de unidades cifradas

En Kaspersky Security Center, puede ver detalles sobre las unidades cifradas y sobre los dispositivos en los que se ha aplicado el cifrado de unidad completa. Si descifra la información de una unidad, la unidad desaparecerá de la lista automáticamente.

*Para ver la lista de unidades cifradas:*

En el menú principal, vaya a **Operaciones** → **Protección y cifrado de datos** → **Unidades cifradas**.

Si la sección no aparece en el menú, significa que está oculta. En la configuración de la interfaz de usuario, habilite la opción **Mostrar protección y cifrado de datos** para mostrar la sección.

Puede exportar la lista de unidades cifradas a un archivo CSV o TXT. Para hacerlo, haga clic en el botón **Exportar a CSV** o **Exportar a TXT**.

## Ver la lista de eventos de cifrado

Al ejecutar tareas de cifrado y descifrado de datos en los dispositivos cliente, Kaspersky Endpoint Security para Windows envía a Kaspersky Security Center información sobre los siguientes tipos de eventos:

- No se puede cifrar o descifrar un archivo o crear un archivo cifrado debido a que falta espacio en disco.
- No se puede cifrar o descifrar un archivo o crear un archivo cifrado debido a problemas de licencia.
- No se puede cifrar o descifrar un archivo o crear un archivo cifrado debido a que faltan derechos de acceso.
- Se ha prohibido el acceso de la aplicación a un archivo cifrado.
- Errores desconocidos.

*Para ver una lista de eventos que se produjeron al cifrar datos en dispositivos:*

En el menú principal, vaya a **Operaciones** → **Protección y cifrado de datos** → **Eventos de cifrado**.

Si la sección no aparece en el menú, significa que está oculta. En la configuración de la interfaz de usuario, habilite la opción **Mostrar protección y cifrado de datos** para mostrar la sección.

Puede exportar la lista de unidades cifradas a un archivo CSV o TXT. Para hacerlo, haga clic en el botón **Exportar a CSV** o **Exportar a TXT**.

También puede examinar la lista de eventos de cifrado para cada dispositivo administrado.

*Para ver los eventos de cifrado de un dispositivo administrado:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.
2. Haga clic en el nombre de un dispositivo administrado.
3. En la pestaña **General**, seleccione la sección **Protección**.
4. Haga clic en el enlace **Ver errores de cifrado de datos**.

# Crear y ver informes de cifrado

Puede generar los siguientes informes:

- Informe sobre el estado de cifrado de los dispositivos administrados. Este informe proporciona detalles sobre el cifrado de datos de varios dispositivos administrados. Por ejemplo, el informe muestra el número de dispositivos a los que se aplica la directiva con reglas de cifrado configuradas. Además, puede averiguar, entre otras cosas, cuántos dispositivos deben reiniciarse. El informe también contiene información sobre la tecnología de cifrado y el algoritmo usados en cada dispositivo.

- Informe sobre el estado de cifrado de los dispositivos de almacenamiento masivo. Este informe contiene la misma información que el informe sobre el estado de cifrado de los dispositivos administrados, pero proporciona datos solo para dispositivos de almacenamiento masivo y unidades extraíbles.

- Informe sobre derechos de acceso a unidades cifradas. Este informe muestra qué cuentas de usuario tienen acceso a unidades cifradas.

- Informe sobre los errores de cifrado de archivos. Este informe contiene información sobre errores que ocurrieron durante tareas de cifrado o descifrado de datos en dispositivos.

- Informe sobre el bloqueo de acceso a los archivos cifrados. Este informe contiene información sobre el bloqueo de acceso de las aplicaciones a los archivos cifrados. Este informe es útil si un usuario o una aplicación no autorizados intenta obtener acceso a archivos o unidades cifradas.

Puede generar cualquiera de los informes en la sección **Supervisión e informes** → **Informes**. También puede generar los siguientes informes de cifrado en la sección **Operaciones** → **Protección y cifrado de datos**:

- Informe sobre el estado de cifrado de los dispositivos de almacenamiento masivo

- Informe sobre derechos de acceso a unidades cifradas

- Informe sobre los errores de cifrado de archivos

*Para generar un informe de cifrado en la sección **Protección y cifrado de datos**:*

1. Verifique que la opción **Mostrar protección y cifrado de datos** esté habilitada en las opciones de la interfaz.

2. En las propiedades de la directiva, abra la pestaña **Configuración de eventos**.

3. En la sección **Crítico**, haga clic en **Agregar evento** y seleccione la casilla junto al evento *Error al implementar las reglas de cifrado o descifrado de archivos*.

4. Haga clic en **Aceptar**.

5. En el menú principal, vaya a **Operaciones** → **Protección y cifrado de datos**.

6. Seleccione una de las siguientes secciones:

   - **Unidades cifradas** genera el informe sobre el estado de cifrado de los dispositivos de almacenamiento masivo o el informe sobre derechos de acceso a unidades cifradas.

   - **Eventos de cifrado** genera el informe sobre los errores de cifrado de archivos.

7. Haga clic en el nombre del informe que desea generar.

Se inicia la generación del informe.

## Brindar acceso a una unidad cifrada en modo sin conexión

Un usuario puede solicitar acceso a un dispositivo cifrado si, por ejemplo, Kaspersky Endpoint Security para Windows no está instalado en el dispositivo administrado. Si recibe una solicitud de acceso, puede crear un archivo de clave de acceso y enviárselo al usuario. Todos los casos de uso y las instrucciones detalladas se proporcionan en la Ayuda de Kaspersky Endpoint Security para Windows.

*Para conceder acceso a una unidad cifrada en modo sin conexión:*

1. Obtenga un archivo de solicitud de acceso de un usuario (un archivo con la extensión FDERTC). Siga las instrucciones de la Ayuda de Kaspersky Endpoint Security para Windows para generar el archivo en Kaspersky Endpoint Security para Windows.

2. En el menú principal, vaya a **Operaciones** → **Protección y cifrado de datos** → **Unidades cifradas**.

   Aparece una lista de unidades cifradas.

3. Seleccione la unidad a la que el usuario haya solicitado acceso.

4. Haga clic en el botón **Otorgar acceso al dispositivo en modo sin conexión**:

5. En la ventana que se abre, seleccione el complemento correspondiente a la aplicación de Kaspersky que se haya utilizado para cifrar la unidad seleccionada.

   > Si una unidad está cifrada con una aplicación de Kaspersky que no es compatible con Kaspersky Security Center Web Console, utilice la Consola de administración basada en Microsoft Management Console para conceder el acceso sin conexión.

6. Siga las instrucciones proporcionadas en la Ayuda de Kaspersky Endpoint Security para Windows (consulte los bloques de expansión al final de la sección).

Tras hacerlo, el usuario aplica el archivo recibido para acceder a la unidad cifrada y leer los datos almacenados en la unidad.

# Usuarios y roles de usuario

En esta sección se explica qué son, cómo se crean y cómo se modifican los usuarios y los roles de usuario. También se brindan instrucciones para asignar roles y grupos a los usuarios y para asociar los roles a perfiles de directivas.

# Acerca de los roles de usuario

Un *rol de usuario* (también denominado *rol*) es un objeto que contiene un conjunto de derechos y privilegios. Un rol puede asociarse a la configuración de las aplicaciones de Kaspersky instaladas en un dispositivo de usuario. Puede asignar un rol a un conjunto de usuarios o a un conjunto de grupos de seguridad en cualquier nivel en la jerarquía de grupos de administración, Servidores de administración, o al nivel de objetos específicos.

Si administra dispositivos a través de una jerarquía de Servidores de administración que incluye servidores de administración virtuales, tenga en cuenta que puede crear, modificar o eliminar funciones de usuario sólo desde un Servidor de administración físico. Luego, puede propagar las funciones de usuario a los Servidores de administración secundarios, incluidos los virtuales.

Los roles de usuario pueden asociarse a perfiles de directivas. Cuando a un usuario se le asigna un rol, se le conceden los ajustes de seguridad que necesita para cumplir con sus funciones laborales.

Un rol de usuario puede asociarse a los usuarios que trabajan con los dispositivos de un grupo de administración específico.

## Alcance de un rol de usuario

El *alcance de un rol de usuario* es una combinación de usuarios y grupos de administración. Los ajustes asociados a un rol de usuario se aplican únicamente a los dispositivos que pertenecen a los usuarios que tienen ese rol, y solo cuando esos dispositivos pertenecen a grupos y subgrupos asociados al rol en cuestión.

## Ventajas de utilizar roles

Una ventaja de utilizar roles es que evita la necesidad de especificar los ajustes de seguridad de cada dispositivo administrado o de cada usuario por separado. La cantidad de dispositivos y usuarios en una empresa puede ser significativa, pero el número de roles laborales que necesitará de ajustes de seguridad especiales siempre será notablemente menor.

## Diferencias con los perfiles de directivas

Los perfiles de directivas son propiedades de una directiva creada para cada aplicación de Kaspersky por separado. Un rol se asocia a muchos perfiles de directivas creados para aplicaciones diferentes. De ese modo, un rol es una manera de unir en un solo lugar los ajustes para un determinado tipo de usuario.

# Ver cuentas y sesiones de usuario

Kaspersky Security Center le permite administrar cuentas de usuario y grupos de cuentas. La aplicación admite dos tipos de cuentas:

- Cuentas de empleados de la organización. El Servidor de administración obtiene datos de las cuentas de estos usuarios cuando sondea la red de la organización.
- Cuentas de usuarios internos. Estas se dan cuando se administran Servidores de administración virtuales. Las cuentas de usuarios internos se crean y utilizan solo para trabajar dentro de Kaspersky Security Center.

Puede consultar la lista de cuentas y sesiones de usuario de una de las siguientes maneras:

- En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos**.
- En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados** → Vínculo del <nombre del dispositivo> → Pestaña **General** → Sección **General** → Bloque **Sesiones**.

  En la sección **Sesiones**, se muestran las cuentas de usuario con sesiones activas en dispositivos con Windows.

La lista de cuentas y sesiones de usuario se muestra correctamente si se cumplen los siguientes requisitos:

- Utilice un Agente de red de la misma versión que el Servidor de Administración o una versión posterior.
- El sondeo de Active Directory debe estar habilitado para mostrar las cuentas de los usuarios del dominio.
- En dispositivos administrados con Windows, el servicio del **Servidor** (**LanmanServer**) está en ejecución.

# Configurar los derechos de acceso a las funciones de la aplicación. Control de acceso basado en roles

Kaspersky Security Center proporciona funciones para el acceso basado en roles a las funciones de Kaspersky Security Center y a las de las aplicaciones de Kaspersky administradas.

Puede configurar los derechos de acceso a las funciones de la aplicación para los usuarios de Kaspersky Security Center de una de las siguientes formas:

- Configure los derechos de cada usuario o grupo de usuarios individualmente;
- puede crear roles de usuario estándares con un conjunto de derechos predefinidos y, luego, puede asignar esos roles a sus usuarios basándose en las responsabilidades de esas personas.

Aplicar roles de usuario es una manera de simplificar y agilizar la tarea rutinaria de configurar derechos de acceso a las funciones de la aplicación. Cada rol tiene asignados permisos de acceso que responden a las tareas y obligaciones con las que deben cumplir los usuarios.

Los roles de usuario pueden llevar nombres que identifiquen sus propósitos. Puede crear un número ilimitado de roles en la aplicación.

Puede utilizar roles de usuario predefinidos, que vienen configurados con un conjunto de derechos, o puede crear roles nuevos y configurar los derechos necesarios por su cuenta.

## Derechos de acceso a las funciones de la aplicación

En la siguiente tabla, se muestran las funciones de Kaspersky Security Center con los derechos de acceso para administrar las tareas, los informes y las configuraciones asociados y para realizar las acciones del usuario asociadas.

Para realizar las acciones de usuario que se detallan en la tabla, el usuario debe tener el derecho indicado junto a la acción.

Los derechos **Leer**, **Modificar**y **Ejecutar**son aplicables a cualquier tarea, informe o ajuste de configuración. Además de estos derechos, un usuario debe tener el derecho **Realizar operaciones en selecciones de dispositivos** para administrar tareas, informes o configuraciones en selecciones de dispositivos.

Todas las tareas, informes, configuraciones y paquetes de instalación que faltan en la tabla pertenecen al área funcional de **Características generales: Funcionalidad básica**.

Derechos de acceso a las funciones de la aplicación

| Área funcional | Derecho | Acción del usuario: derecho necesario para realizar la acción | Tarea | Informe | Otro |
|---|---|---|---|---|---|
| **Características generales**: **Gestión de grupos de administración** | **Modificar** | • Agregar un dispositivo a un grupo de administración: **Modificar**<br>• Eliminar un dispositivo de un grupo de administración: **Modificar**<br>• Agregar un grupo de administración a otro grupo de administración: **Modificar**<br>• Eliminar un grupo de administración de otro grupo de administración: **Modificar** | Ninguno | N/C | N/C |
| **Características generales**: **Acceder a objetos sin importar sus ACL** | **Leer** | Obtener acceso Leer a todos los objetos: **Leer** | Ninguno | N/C | El área funcional **Características generales: Acceder a objetos sin importar sus ACL** está diseñada con fines de auditoría. Cuando los usuarios obtienen derechos de **Leer** en esta área funcional, obtienen acceso de **Leer** completo a todos los objetos y pueden ejecutar cualquier tarea creada en selecciones de dispositivos conectados al Servidor de administración a través del Agente de red con derechos de administrador local (root para Linux). Recomendamos conceder estos derechos con precaución y a un conjunto limitado de usuarios que los necesiten para realizar sus funciones oficiales.<br>El acceso se otorga sin importar los demás derechos, incluso si se prohíbe el acceso Leera objetos específicos. |

| Área funcional | Derecho | Acción del usuario: derecho necesario para realizar la acción | Tarea | Informe | Otro |
|---|---|---|---|---|---|
| **Características generales**: **Funcionalidad básica** | • **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Realizar operaciones en selecciones de dispositivos** | • Reglas de movimiento de dispositivos (crear, modificar o eliminar) para el Servidor virtual: **Modificar**, **Realizar operaciones en selecciones de dispositivos**<br>• Obtener certificado personalizado del protocolo móvil (LWNGT): **Leer**<br>• Establecer certificado personalizado del protocolo móvil (LWNGT): **Modificar**<br>• Obtener la lista de redes definidas por NLA: **Leer**<br>• Agregar, modificar o eliminar la lista de redes definidas por NLA: **Modificar**<br>• Ver la lista de control de acceso de los grupos: **Leer**<br>• Ver el registro de eventos de Kaspersky: **Leer**<br>• Ver la clave de recuperación para restaurar el acceso a un disco duro cifrado con BitLocker: **Ejecutar** | • "Descargar actualizaciones en el repositorio del Servidor de administración"<br>• "Entregar informes"<br>• "Distribuir paquete de instalación"<br>• "Instalar aplicación en Servidores de administración secundarios de forma remota" | • "Informe del estado de la protección"<br>• "Informe de amenazas"<br>• "Informe de los dispositivos más infectados"<br>• "Informe sobre el estado de las bases de datos antivirus"<br>• "Informe de errores"<br>• "Informe de ataques de red"<br>• "Informe conciso sobre las aplicaciones instaladas para la protección de sistemas de correo"<br>• "Informe conciso sobre las aplicaciones instaladas para la defensa del perímetro"<br>• "Informe conciso sobre los tipos de aplicaciones instaladas"<br>• "Informe sobre usuarios de dispositivos infectados"<br>• "Informe sobre incidentes"<br>• "Informe de eventos"<br>• "Informe de actividad de puntos de distribución"<br>• "Informe sobre los Servidores de administración secundarios"<br>• "Informe sobre los eventos de Control de dispositivos"<br>• "Informe de vulnerabilidades"<br>• "Informe sobre aplicaciones prohibidas"<br>• "Informe de Control web"<br>• "Informe sobre el estado de cifrado de los dispositivos administrados" | Ninguno |

| Área funcional | Derecho | Acción del usuario: derecho necesario para realizar la acción | Tarea | Informe | Otro |
|---|---|---|---|---|---|
| | | | | • "Informe sobre el estado de cifrado de los dispositivos de almacenamiento masivo"<br>• "Informe sobre los errores de cifrado de archivos"<br>• "Informe sobre el bloqueo de acceso a los archivos cifrados"<br>• "Informe sobre derechos de acceso a los dispositivos cifrados"<br>• "Informe sobre permisos de usuario vigentes"<br>• "Informe sobre derechos" | |
| **Características generales**: **Objetos eliminados** | • **Leer**<br>• **Modificar** | • Ver objetos eliminados en la Papelera de reciclaje: **Leer**<br>• Eliminar objetos de la Papelera de reciclaje: **Modificar** | Ninguno | N/C | N/C |
| **Características generales**: **Procesamiento de eventos** | • **Eliminar eventos**<br>• **Editar configuración de notificación de eventos**<br>• **Editar la configuración de registro de eventos**<br>• **Modificar** | • Cambiar los ajustes de registro de eventos: **Editar la configuración de registro de eventos**<br>• Cambiar la configuración de notificaciones de eventos: **Editar configuración de notificación de eventos**<br>• Eliminar eventos: **Eliminar eventos** | Ninguno | N/C | Configuración:<br>• Configuración de brotes de virus: número de detecciones de virus necesarias para crear un evento de brote de virus<br>• Configuración de brotes de virus: período sobre el que se evalúan las detecciones de virus<br>• Cantidad máxima de eventos almacenados en la base de datos<br>• Período por el que se almacenan los eventos de los dispositivos eliminados |

| Área funcional | Derecho | Acción del usuario: derecho necesario para realizar la acción | Tarea | Informe | Otro |
|---|---|---|---|---|---|
| **Características generales**: Operaciones en el Servidor de administración | • **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Modificar ACL de objeto**<br>• **Realizar operaciones en selecciones de dispositivos** | • Especificar los puertos del Servidor de administración para la conexión del Agente de red: **Modificar**<br>• Especificar los puertos del proxy de activación ejecutado en el Servidor de administración: **Modificar**<br>• Especificar los puertos del proxy de activación para dispositivos móviles ejecutado en el Servidor de administración: **Modificar**<br>• Especificar los puertos del Servidor web para la distribución de paquetes independientes: **Modificar**<br>• Especificar los puertos del Servidor web para la distribución de perfiles de MDM: **Modificar**<br>• Especificar los puertos SSL del Servidor de administración para la conexión a través de Kaspersky Security Center Web Console: **Modificar**<br>• Especificar los puertos del Servidor de administración para la conexión de dispositivos móviles: **Modificar**<br>• Especificar la cantidad máxima de eventos que se pueden almacenar en la base de datos del Servidor de administración: **Modificar**<br>• Especificar la cantidad máxima de eventos que puede enviar el Servidor de administración: **Modificar**<br>• Especificar el período durante el cual puede enviar eventos el Servidor de administración: **Modificar** | • "Copia de seguridad de los datos del Servidor de administración"<br>• "Mantenimiento de bases de datos" | Ninguno | N/C |

| Área funcional | Derecho | Acción del usuario: derecho necesario para realizar la acción | Tarea | Informe | Otro |
|---|---|---|---|---|---|
| **Características generales**: **Despliegue de la aplicación de Kaspersky** | • **Administrar parches de Kaspersky**<br>• **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Realizar operaciones en selecciones de dispositivos** | Aprobar o rechazar la instalación del parche: **Administrar parches de Kaspersky** | Ninguno | • "Informe sobre el uso de claves de licencia por Servidor de administración virtual"<br>• "Informe de versiones del software de Kaspersky"<br>• "Informe de aplicaciones incompatibles"<br>• "Informe sobre la versión de las actualizaciones para los módulos de software de Kaspersky"<br>• "Informe del despliegue de la protección" | Paquete de instalación: "Kaspersky" |
| **Características generales**: **Administración de claves de licencia** | • **Exportar archivo de clave**<br>• **Modificar** | • Exportar un archivo de clave: **Exportar archivo de clave**<br>• Modificar la configuración de la clave de licencia del Servidor de administración: **Modificar** | Ninguno | N/C | N/C |
| **Características generales**: **Administración de informes controlada** | • **Leer**<br>• **Modificar** | • Crear informes independientemente de sus ACL: **Modificar**<br>• Ejecutar informes independientemente de sus ACL: **Leer** | Ninguno | N/C | N/C |
| **Características generales**: **Jerarquía de Servidores de administración** | **Configurar la jerarquía de Servidores de administración** | Registrar, actualizar o eliminar Servidores de administración secundarios: **Configurar la jerarquía de Servidores de administración** | Ninguno | N/C | N/C |

| Área funcional | Derecho | Acción del usuario: derecho necesario para realizar la acción | Tarea | Informe | Otro |
|---|---|---|---|---|---|
| **Características generales**: **Permisos de usuario** | **Modificar ACL de objeto** | • Cambiar las propiedades de seguridad de cualquier objeto: **Modificar ACL de objeto**<br>• Administrar roles de usuario: **Modificar ACL de objeto**<br>• Administrar usuarios internos: **Modificar ACL de objeto**<br>• Administrar grupos de seguridad: **Modificar ACL de objeto**<br>• Administrar alias: **Modificar ACL de objeto** | Ninguno | N/C | N/C |
| **Características generales**: **Servidores de administración virtuales** | • **Administrar Servidores de administración virtuales**<br>• **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Realizar operaciones en selecciones de dispositivos** | • Obtener la lista de Servidores de administración virtuales: **Leer**<br>• Obtener información sobre el Servidor de administración virtual: **Leer**<br>• Crear, actualizar o eliminar un Servidor de administración virtual: **Administrar Servidores de administración virtuales**<br>• Mover un Servidor de administración virtual a otro grupo: **Administrar Servidores de administración virtuales**<br>• Definir los permisos de un Servidor de administración virtual: **Administrar Servidores de administración virtuales** | Ninguno | "Informe sobre los resultados de la instalación de actualizaciones de software de terceros" | Ninguno |
| **Características generales**: **Administración de claves de cifrado** | **Modificar** | Importar las claves de cifrado: **Modificar** | Ninguno | N/C | N/C |

| Área funcional | Derecho | Acción del usuario: derecho necesario para realizar la acción | Tarea | Informe | Otro |
|---|---|---|---|---|---|
| **Administración de dispositivos móviles: General** | • **Conectar nuevos dispositivos**<br>• **Enviar únicamente comandos de información a dispositivos móviles**<br>• **Enviar comandos a dispositivos móviles**<br>• **Administrar certificados**<br>• **Leer**<br>• **Modificar** | • Obtener datos de restauración del servicio de administración de claves: **Leer**<br>• Eliminar certificados de usuario: **Administrar certificados**<br>• Obtener la parte pública de un certificado de usuario: **Leer**<br>• Comprobar si la infraestructura de claves públicas está habilitada: **Leer**<br>• Comprobar la cuenta de la infraestructura de claves públicas: **Leer**<br>• Obtener plantillas de la infraestructura de claves públicas: **Leer**<br>• Obtener plantillas de la infraestructura de claves públicas mediante un certificado de uso extendido de clave: **Leer**<br>• Comprobar si el certificado de la infraestructura de claves públicas fue revocado: **Leer**<br>• Actualizar la configuración de emisión de certificados de usuario: **Administrar certificados**<br>• Obtener la configuración de emisión de certificados de usuario: **Leer**<br>• Obtener paquetes por nombre y versión de aplicación: **Leer**<br>• Definir o cancelar un certificado de usuario: **Administrar certificados**<br>• Renovar un certificado de usuario: **Administrar certificados**<br>• Definir una etiqueta para un certificado de usuario: **Administrar certificados**<br>• Ejecutar la generación del paquete de instalación de MDM; cancelar la | Ninguno | N/C | N/C |

| Área funcional | Derecho | Acción del usuario: derecho necesario para realizar la acción | Tarea | Informe | Otro |
|---|---|---|---|---|---|
| | | generación del paquete de instalación de MDM: **Conectar nuevos dispositivos** | | | |
| **Administración de sistemas: Conectividad** | • **Iniciar sesiones RDP**<br>• **Conexión a sesiones de RDP existentes**<br>• **Iniciar la tunelización**<br>• **Guardar archivos de los dispositivos en la estación de trabajo del administrador**<br>• **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Realizar operaciones en selecciones de dispositivos** | • Crear sesión de escritorio compartido: **Iniciar sesiones RDP**<br>• Crear una sesión de RDP: **Conexión a sesiones de RDP existentes**<br>• Crear un túnel: **Iniciar la tunelización**<br>• Guardar la lista de red de contenido: **Guardar archivos de los dispositivos en la estación de trabajo del administrador** | Ninguno | "Informe sobre los usuarios de los dispositivos" | Ninguno |
| **Administración de sistemas: Inventario de hardware** | • **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Realizar operaciones en selecciones de dispositivos** | • Obtener o exportar un objeto del inventario de hardware: **Leer**<br>• Agregar, definir o eliminar un objeto del inventario de hardware: **Modificar** | Ninguno | • "Informe sobre el registro de hardware"<br>• "Informe sobre los cambios en la configuración"<br>• "Informe de hardware" | Ninguno |
| **Administración de sistemas: Control de acceso a la red** | • **Leer**<br>• **Modificar** | • Ver la configuración de CISCO: **Leer**<br>• Cambiar la configuración de CISCO: **Modificar** | Ninguno | N/C | N/C |
| **Administración de sistemas: Despliegue de sistemas operativos** | • **Desplegar servidores PXE**<br>• **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Realizar operaciones en selecciones de dispositivos** | • Desplegar servidores PXE: **Desplegar servidores PXE**<br>• Ver una lista de servidores PXE: **Leer**<br>• Iniciar o detener el proceso de instalación en clientes PXE: **Ejecutar**<br>• Administrar controladores para WinPE e imágenes de sistema operativo: **Modificar** | "Crear un paquete de instalación con la imagen del SO de un dispositivo de referencia" | Ninguno | Paquete de instalación: "Imagen del SO" |

| Área funcional | Derecho | Acción del usuario: derecho necesario para realizar la acción | Tarea | Informe | Otro |
|---|---|---|---|---|---|
| **Administración de sistemas: Administración de vulnerabilidades y parches** | • **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Realizar operaciones en selecciones de dispositivos** | • Ver propiedades de parches de terceros: **Leer**<br>• Cambiar las propiedades de parches de terceros: **Modificar** | • "Sincronización con Windows Update"<br>• "Instalar actualizaciones de Windows Update"<br>• "Reparar vulnerabilidades"<br>• "Instalar actualizaciones requeridas y reparar vulnerabilidades" | "Informe de actualizaciones de software" | Ninguno |
| **Administración de sistemas: Instalación remota** | • **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Realizar operaciones en selecciones de dispositivos** | • Ver las propiedades de un paquete de instalación de una aplicación de terceros (con Administración de vulnerabilidades y parches habilitada): **Leer**<br>• Cambiar las propiedades de un paquete de instalación de una aplicación de terceros (con Administración de vulnerabilidades y parches habilitada): **Modificar** | Ninguno | N/C | Paquetes de instalación:<br>• "Aplicación personalizada"<br>• "Paquete VAPM" |

| Área funcional | Derecho | Acción del usuario: derecho necesario para realizar la acción | Tarea | Informe | Otro |
|---|---|---|---|---|---|
| **Administración de sistemas: Inventario de software** | • **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Realizar operaciones en selecciones de dispositivos** | Ninguno | N/C | • "Informe sobre aplicaciones instaladas"<br>• "Informe del historial del registro de aplicaciones"<br>• "Informe sobre el estado de los grupos de aplicaciones con licencia"<br>• "Informe sobre claves de licencia de software de terceros" | Ninguno |
| **Administración de sistemas: Ejecutar scripts de forma remota** | • **Leer**<br>• **Modificar**<br>• **Ejecutar**<br>• **Realizar operaciones en selecciones de dispositivos** | El usuario puede ver las propiedades de la tarea: **Leer**<br>El usuario puede crear, eliminar o modificar un paquete de instalación: **Modificar**<br>El usuario puede ejecutar una tarea: **Modificar** En los dispositivos cliente Linux, los scripts se ejecutan con privilegios de raíz.<br>El usuario puede ejecutar una tarea o programar su ejecución: **Ejecutar**<br>El usuario puede ejecutar una tarea en una selección de dispositivos: **Realizar operaciones en selecciones de dispositivos** | "Ejecución remota de scripts" | Ninguno | N/C |

## Roles de usuario predefinidos

Los roles de usuario asignados a los usuarios de Kaspersky Security Center les brindan los conjuntos de derechos que necesitan para acceder a las funciones de la aplicación.

A los usuarios creados en un Servidor virtual no se les puede asignar una función en el Servidor de administración.

Puede utilizar roles de usuario predefinidos, que vienen configurados con un conjunto de derechos, o puede crear roles nuevos. En este caso, debe establecer el alcance del rol y asignar los derechos de acceso a las funciones de Kaspersky Security Center por su cuenta. Algunos de los roles predefinidos de Kaspersky Security Center se pueden asociar con puestos de trabajo específicos; es el caso, por ejemplo, de los roles **Auditor**, **Supervisor** y **Director de seguridad**, que han estado disponibles en Kaspersky Security Center desde la versión 11. Los derechos de acceso de estos roles están preconfigurados para facilitar las obligaciones y las tareas típicas de los puestos asociados. En la siguiente tabla, se muestra cómo estos roles pueden vincularse a puestos de trabajo específicos.

Ejemplos de roles para puestos de trabajo específicos

| Rol | Comentario |
|---|---|
| Auditor | Permite todas las operaciones de visualización y ejecución de las tareas creadas en selecciones de dispositivos conectados al Servidor de administración a través del Agente de red con derechos de administrador local (raíz para Linux).<br><br>Recomendamos asignar esta función con cuidado y a un grupo limitado de usuarios que la necesiten para desempeñar sus funciones oficiales. |
| Supervisor | Permite realizar cualquier operación de visualización; no permite realizar otras operaciones. Puede asignar este rol a un oficial de seguridad y a otras personas que tengan a su cargo la seguridad de TI de la organización. |
| Oficial de seguridad | Permite realizar cualquier operación de visualización y permite administrar los informes; también otorga permisos limitados en el área **Administración de sistemas**: **Conectividad**. Puede asignar este rol al responsable de la seguridad de TI de su organización. |

En la siguiente tabla, se muestran los derechos de acceso asignados a cada rol de usuario predefinido.

Derechos de acceso de los roles de usuario predefinidos

| Rol | Descripción |
|---|---|
| Administrador del Servidor de administración | Permite todas las operaciones en las siguientes áreas funcionales:<br>• **Características generales**:<br>  • **Funcionalidad básica**<br>  • **Procesamiento de eventos**<br>  • **Jerarquía de Servidores de administración**<br>  • **Servidores de administración virtuales**<br>• **Administración de sistemas**:<br>  • **Conectividad**<br>  • **Inventario de hardware**<br>  • **Inventario de software**<br><br>Otorga los derechos **Leer** y **Escribir** en el área funcional **Características generales: Administración de claves de cifrado**. |
| Operador del Servidor de administración | Otorga los derechos **Leer** y **Ejecutar** en las siguientes áreas funcionales:<br>• **Características generales**:<br>  • **Funcionalidad básica**<br>  • **Servidores de administración virtuales**<br>• **Administración de sistemas**:<br>  • **Conectividad**<br>  • **Inventario de hardware**<br>  • **Inventario de software** |
| Auditor | Permite todas las operaciones en todas las áreas funcionales, en **Características generales**:<br>• **Acceder a objetos sin importar sus ACL**<br>• **Objetos eliminados**<br>• **Administración de informes controlada**<br><br>Puede asignar este rol a la persona que realiza la auditoría de su organización. |

| Rol | Descripción |
| --- | --- |
| Administrador de instalación | Permite todas las operaciones en las siguientes áreas funcionales:<br>• **Características generales**:<br>  • **Funcionalidad básica**<br>  • **Despliegue del software de Kaspersky**<br>  • **Administración de claves de licencia**<br>• **Administración de sistemas**:<br>  • **Despliegue del sistema operativo**<br>  • **Administración de vulnerabilidades y parches**<br>  • **Instalación remota**<br>  • **Inventario de software**<br>Otorga los derechos **Leer** y **Ejecutar** en el área funcional **Características generales: Servidores de administración virtuales**. |
| Operador de instalación | Otorga los derechos **Leer** y **Ejecutar** en las siguientes áreas funcionales:<br>• **Características generales**:<br>  • **Funcionalidad básica**<br>  • **Despliegue del software de Kaspersky** (también otorga el derecho **Administrar parches de Kaspersky** en esta área)<br>  • **Servidores de administración virtuales**<br>• **Administración de sistemas**:<br>  • **Despliegue del sistema operativo**<br>  • **Administración de vulnerabilidades y parches**<br>  • **Instalación remota**<br>  • **Inventario de software** |
| Administrador de Kaspersky Endpoint Security | Permite todas las operaciones en las siguientes áreas funcionales:<br>• **Características generales: funcionalidad básica**<br>• Área de Kaspersky Endpoint Security (se incluyen todas las funciones)<br>Otorga los derechos **Leer** y **Escribir** en el área funcional **Características generales: Administración de claves de cifrado**. |
| Operador de Kaspersky Endpoint Security | Otorga los derechos **Leer** y **Ejecutar** en las siguientes áreas funcionales:<br>• **Características generales: funcionalidad básica**<br>• Área de Kaspersky Endpoint Security (se incluyen todas las funciones) |
| Administrador principal | Permite todas las operaciones en todas las áreas funcionales, *excepto* en las siguientes áreas, en **Características generales**:<br>• **Acceder a objetos sin importar sus ACL**<br>• **Administración de informes forzados**<br>Otorga los derechos **Leer** y **Escribir** en el área funcional **Características generales: Administración de claves de cifrado**. |

| Rol | Descripción |
| --- | --- |
| Operador principal | Otorga los derechos **Leer** y **Ejecutar** (cuando corresponde) en las siguientes áreas funcionales:<br>• **Características generales**:<br>  • **Funcionalidad básica**<br>  • **Objetos eliminados**<br>  • **Operaciones en el Servidor de administración**<br>  • **Despliegue de la aplicación de Kaspersky**<br>  • **Servidores de administración virtuales**<br>• **Administración de dispositivos móviles: General**<br>• **Administración de sistemas** (se incluyen todas las funciones)<br>• Área de Kaspersky Endpoint Security (se incluyen todas las funciones) |
| Administrador de Administración de dispositivos móviles | Permite todas las operaciones en las siguientes áreas funcionales:<br>• **Características generales: funcionalidad básica**<br>• **Administración de dispositivos móviles: General** |
| Operador de Administración de dispositivos móviles | Otorga los derechos **Leer** y **Ejecutar** en el área funcional **Características generales**: **Funcionalidad básica**.<br>Otorga los derechos **Leer** y **Enviar únicamente comandos de información a dispositivos móviles** en **Administración de dispositivos móviles**: **General** área funcional: |
| Director de seguridad | Permite todas las operaciones en las siguientes áreas funcionales, en **Características generales**:<br>• **Acceder a objetos sin importar sus ACL**<br>• **Administración de informes controlada**<br>Otorga los derechos **Leer**, **Escribir**, **Ejecutar**, **Guardar archivos de los dispositivos en la estación de trabajo del administrador** y **Realizar operaciones en selecciones de dispositivos** en el área funcional **Administración de sistemas: Conectividad**.<br>Puede asignar este rol al responsable de la seguridad de TI de su organización. |
| Usuario de Self Service Portal | Permite todas las operaciones en el área funcional **Administración de dispositivos móviles: Self Service Portal**. Esta función no es compatible con Kaspersky Security Center 11 ni versiones posteriores. |
| Supervisor | Otorga el derecho **Leer** en las áreas funcionales **Características generales**: **Acceder a objetos sin importar sus ACL** y **Características generales**: **Administración de informes controlada**.<br>Puede asignar este rol a un Director de seguridad y a otras personas que tengan a su cargo la seguridad de TI de la organización. |
| Administrador de Administración de vulnerabilidades y parches | Permite todas las operaciones en las áreas funcionales **Características generales**: **Funcionalidad básica** y **Administración de sistemas** (se incluyen todas las funciones). |
| Operador de Administración de vulnerabilidades y parches | Otorga los derechos **Leer** y **Ejecutar** (cuando corresponde) en las áreas funcionales **Características generales**: **Funcionalidad básica** y **Administración de sistemas** (se incluyen todas las funciones). |

## Asignación de derechos de acceso a objetos específicos

Además de asignar derechos de acceso al nivel de servidor, puede configurar el acceso a objetos específicos, por ejemplo, a una tarea específica. La aplicación le permite especificar derechos de acceso a los siguientes tipos de objetos:

- Grupos de administración
- Tareas
- Informes

- Selecciones de dispositivos
- Selecciones de eventos

*Para asignar derechos de acceso a un objeto específico:*

1. Según el tipo de objeto, en el menú principal vaya a la sección correspondiente:
   - **Activos (dispositivos) → Jerarquía de grupos**
   - **Activos (dispositivos) → Tareas**
   - **Supervisión e informes → Informes**
   - **Activos (dispositivos) → Selecciones de dispositivos**
   - **Supervisión e informes → Selecciones de eventos**
2. Abra las propiedades del objeto al que desea configurar los derechos de acceso.

   Para abrir la ventana de propiedades de un grupo de administración o una tarea, haga clic en el nombre del objeto. Las propiedades de otros objetos se pueden abrir usando el botón en la barra de herramientas.
3. En la ventana de propiedades, abra la sección **Derechos de acceso**.

   Se abre la lista de usuarios. Los usuarios y grupos de seguridad enumerados tienen derechos de acceso al objeto. De forma predeterminada, si utiliza una jerarquía de grupos o servidores de administración, la lista y los derechos de acceso se heredan del grupo de administración principal o del servidor principal.
4. Para poder modificar la lista, habilite la opción **Usar permisos personalizados** opción.
5. Configurar derechos de acceso:
   - Use los botones **Agregar** y **Eliminar** para modificar la lista.
   - Especifique los derechos de acceso para un usuario o grupo de seguridad. Realice una de las siguientes acciones:
     - Si desea especificar los derechos de acceso manualmente, seleccione el usuario o grupo de seguridad, haga clic en el botón **Derechos de acceso** y, a continuación, especifique los derechos de acceso.
     - Si desea asignar un rol de usuario al usuario o grupo de seguridad, seleccione el usuario o grupo de seguridad, haga clic en el botón **Roles** y, a continuación, seleccione el rol que desea asignar.
6. Haga clic en el botón **Guardar**.

Los derechos de acceso al objeto se configuran.

## Asignar derechos de acceso a usuarios y grupos de seguridad

Puede asignar derechos de acceso a sus usuarios y grupos de seguridad para que puedan utilizar diferentes funciones del Servidor de administración, como Kaspersky Endpoint Security for Linux.

*Para asignar derechos de acceso a un usuario o grupo de seguridad, haga lo siguiente:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Derechos de acceso**, marque la casilla ubicada junto al nombre del usuario o del grupo de seguridad al que desea asignar derechos y, luego, haga clic en el botón **Derechos de acceso**.

   No puede seleccionar varios usuarios o grupos de seguridad al mismo tiempo. Si selecciona más de un elemento, el botón **Derechos de acceso** se deshabilitará.

3. Configure el conjunto de derechos para el usuario o grupo:

   a. Amplíe el nodo con funciones del Servidor de administración o de otra aplicación de Kaspersky.

   b. Marque las casillas **Permitir** o **Denegar** ubicadas junto a la función o el derecho de acceso pertinentes.

      *Ejemplo 1:* Marque la casilla **Permitir** ubicada junto al nodo **Integración de aplicaciones** para otorgar a un usuario o grupo todos los derechos de acceso disponibles para la característica de integración de aplicaciones (**Lectura**, **Escritura** y **Ejecución**).

      *Ejemplo 2:* Expanda el nodo **Administración de claves de cifrado** y marque la casilla **Permitir** ubicada junto al permiso **Escritura** para otorgar a un usuario o grupo el derecho de acceso **Escritura** para la función de administración de claves de cifrado.

4. Después de configurar el conjunto de derechos de acceso, haga clic en **Aceptar**.

Se configurará el conjunto de derechos para el usuario o grupo de usuarios.

Los permisos del Servidor de administración (o el grupo de administración) se dividen en las siguientes áreas:

- Características generales:
  - Gestión de grupos de administración
  - Acceder a objetos sin importar sus ACL
  - Funcionalidad básica
  - Objetos eliminados
  - Administración de claves de cifrado
  - Procesamiento de eventos
  - Operaciones en el Servidor de administración (solo en la ventana de propiedades del Servidor de administración)
  - Etiquetas del dispositivo
  - Despliegue de la aplicación de Kaspersky
  - Administración de claves de licencia
  - Integración de aplicaciones
  - Administración de informes controlada
  - Jerarquía de Servidores de administración
  - Permisos de usuario
  - Servidores de administración virtuales
- Administración de dispositivos móviles:
  - General
  - Self Service Portal
- Administración de sistemas:
  - Conectividad
  - Ejecutar scripts de forma remota
  - Inventario de hardware
  - Control de acceso a la red
  - Despliegue de sistemas operativos
  - Administración de vulnerabilidades y parches

- Instalación remota
- Inventario de software

Si no se selecciona **Permitir** ni **Denegar** para un derecho de acceso, el acceso se considera *indefinido*: el usuario no tendrá ese derecho hasta que se le conceda o deniegue explícitamente.

Los derechos de un usuario son la suma de lo siguiente:

- los propios derechos del usuario
- los derechos de todos los roles asignados al usuario
- los derechos de todo el grupo de seguridad al que pertenece el usuario
- los derechos de todos los roles asignados a los grupos de seguridad a los que pertenece el usuario

Si al menos uno de estos conjuntos de derechos tiene **Denegar** para un permiso, al usuario se le niega este permiso, incluso si otros conjuntos lo permiten o lo dejan sin definir.

También puede agregar usuarios y grupos de seguridad al alcance de un rol de usuario para usar diferentes funciones del Servidor de administración. La configuración asociada a un rol de usuario se aplica únicamente a los dispositivos que pertenecen a los usuarios que tienen ese rol, y solo cuando esos dispositivos pertenecen a grupos y subgrupos asociados al rol en cuestión.

## Agregar una cuenta de un usuario interno

Si desea agregar una cuenta de usuario, asegúrese de que su cuenta tenga el derecho Modificar ACL de objeto en el área funcional Características generales: Permisos de usuario.

*Para agregar una nueva cuenta de usuario interna a Kaspersky Security Center:*

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
2. Haga clic en **Agregar**.

3. En la ventana **Agregar usuario** que se abre, especifique la configuración de la nueva cuenta de usuario:

   - **Nombre**
   - **Contraseña**

     La contraseña debe cumplir con las siguientes reglas:

     - La contraseña debe tener entre 8 y 256 caracteres.
     - La contraseña debe incluir caracteres de al menos tres de los grupos enumerados a continuación:
       - Letras mayúsculas (A-Z)
       - Letras minúsculas (a-z)
       - Números (0-9)
       - Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - La contraseña no debe contener espacios en blanco, caracteres Unicode o la combinación de "." y "@" cuando "." está colocado delante de "@".

     Para ver la contraseña ingresada, haga clic en .

     Puede habilitar la opción **El usuario debe cambiar la contraseña la primera vez que inicie sesión** para obligarlo a cambiar la contraseña cuando se autentique por primera vez.

4. Guarde los cambios para terminar de crear la nueva cuenta de usuario.

Se agrega una nueva cuenta de usuarios a la lista de usuarios.

## Crear un grupo de seguridad

*Para crear un grupo de seguridad:*

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Grupos**.
2. Haga clic en **Agregar**.
3. En la ventana **Crear grupo de seguridad** que se abre, especifique la siguiente configuración para el nuevo grupo de seguridad:

   - **Nombre del grupo**
   - **Descripción**

4. Haga clic en **Guardar** para guardar los cambios.

Se agrega un nuevo grupo de seguridad a la lista de grupos.

# Editar una cuenta de un usuario interno

Si desea editar una cuenta de usuario, asegúrese de que su cuenta tenga el derecho Modificar ACL de objeto en el área funcional Características generales: Permisos de usuario.

*Modificar una cuenta de usuario interna en Kaspersky Security Center:*

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
2. Haga clic en el nombre de la cuenta de usuario que desee editar.

3. En la ventana de configuración de usuario que se abre, en la pestaña **General**, cambie la configuración de la cuenta de usuario:

   - Estado del usuario

     Si es necesario, cambie el botón de alternar a **Deshabilitado** para prohibir que el usuario se conecte a la aplicación. Puede desactivar una cuenta, por ejemplo, después de que un empleado abandone la empresa.

   - **Nombre**
   - **Nombre completo**
   - **Descripción**
   - **Dirección de correo electrónico**
   - **Teléfono principal**
   - Contraseña

     Si es necesario, puede establecer una nueva contraseña para la conexión del usuario a Kaspersky Security Center de la siguiente manera:

     a. Haga clic en el botón **Cambiar contraseña** y establezca la contraseña nueva de la cuenta de usuario.

     La contraseña debe cumplir con las siguientes reglas:

     - La contraseña debe tener entre 8 y 256 caracteres.
     - La contraseña debe incluir caracteres de al menos tres de los grupos enumerados a continuación:
       - Letras mayúsculas (A-Z)
       - Letras minúsculas (a-z)
       - Números (0-9)
       - Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - La contraseña no debe contener espacios en blanco, caracteres Unicode o la combinación de "." y "@" cuando "." está colocado delante de "@".

     Para ver la contraseña ingresada, haga clic en .

     b. Si es necesario, habilite la opción **El usuario debe cambiar la contraseña la primera vez que inicie sesión** para obligarlo a cambiar la contraseña cuando se autentique de nuevo.

     c. Si la cuenta de usuario está protegida contra modificaciones no autorizadas, debe comprobar que tiene permisos para cambiar la cuenta. En la ventana **Protección de cuentas**, especifique las credenciales de la cuenta con derecho de Modificar ACL de objeto en el área funcional Características generales: Permisos de usuario.

4. En la pestaña **Seguridad de autenticación**, puede especificar la configuración de seguridad para esta cuenta.

5. En la pestaña **Grupos**, puede añadir al usuario a grupos de seguridad.
6. En la pestaña **Dispositivos**, puede asignar dispositivos al usuario.
7. En la pestaña **Roles**, puede asignar funciones al usuario.
8. Guarde los cambios para terminar de editar la cuenta de usuario.

La cuenta de usuario actualizada aparece en la lista de usuarios.

## Editar un grupo de seguridad

*Para editar un grupo de seguridad:*

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Grupos**.
2. Haga clic en el nombre del grupo de seguridad que desee editar.
3. Cuando se abra la ventana de configuración del grupo, cambie la configuración del grupo de seguridad:
   - En la pestaña **General**, puede cambiar la configuración de **Nombre** y **Descripción**. Estas configuraciones están disponibles solo para grupos de seguridad internos.
   - En la pestaña **Usuarios**, puede agregar usuarios al grupo de seguridad. Esta configuración solo está disponible para usuarios internos y grupos de seguridad internos.
   - En la pestaña **Roles**, puede asignar un rol al grupo de seguridad.
4. Haga clic en **Guardar** para guardar los cambios.

Los cambios se aplican al grupo de seguridad.

## Asignación de un rol a un usuario o a un grupo de seguridad

*Para asignar un rol a un usuario o grupo de seguridad, haga lo siguiente:*

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos**, y luego seleccione la pestaña **Usuarios** o **Grupos**.
2. Seleccione el nombre del usuario o del grupo de seguridad a quien desea asignar un rol.

   Puede seleccionar varios nombres.
3. En la línea del menú, haga clic en el botón **Asignar rol**.

   Se inicia el asistente de asignación de roles.
4. Siga las instrucciones del asistente: seleccione el rol que desea asignar a los usuarios o grupos de seguridad seleccionados, y elija el alcance del rol.

   El alcance de un rol de usuario es una combinación de usuarios y grupos de administración. Los ajustes asociados a un rol de usuario se aplican únicamente a los dispositivos que pertenecen a los usuarios que tienen ese rol, y solo cuando esos dispositivos pertenecen a grupos y subgrupos asociados al rol en cuestión.

El rol con un conjunto de derechos para trabajar con el Servidor de administración se asigna al usuario (o usuarios, o al grupo de seguridad). En la lista de usuarios o grupos de seguridad, aparece una casilla en la columna **Tiene roles asignados**.

A los usuarios creados en un Servidor virtual no se les puede asignar una función en el Servidor de administración.

## Agregar cuentas de usuario a un grupo interno de seguridad

Las únicas cuentas que se pueden agregar a un grupo interno son las de usuarios de seguridad.

*Para agregar cuentas de usuario a un grupo interno de seguridad:*

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
2. Active las casillas de verificación ubicadas junto a las cuentas de usuario que desee agregar al grupo de seguridad.
3. Haga clic en el botón **Asignar grupo**.
4. En la ventana **Asignar grupo** que se abrirá, seleccione el grupo de seguridad al que desee agregar las cuentas de usuario.
5. Haga clic en el botón **Guardar**.

Las cuentas de usuario se agregarán al grupo de seguridad. También puede agregar usuarios internos a un grupo de seguridad mediante la configuración del grupo.

## Designación de un usuario como propietario de un dispositivo

Si busca información para designar a un usuario como propietario de un dispositivo móvil, consulte la Ayuda de Kaspersky Security para dispositivos móviles.

*Para designar a un usuario como propietario de un dispositivo:*

1. Si desea asignar un propietario de un dispositivo conectado a un Servidor de administración virtual, primero cambie al Servidor de administración virtual:
   a. En el menú principal, haga clic en el ícono de corchete ( ) a la derecha del nombre del Servidor de administración actual.
   b. Seleccione el Servidor de administración requerido.
2. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
   Se abre una lista de usuarios. Si actualmente está conectado a un Servidor de administración virtual, la lista incluye usuarios del Servidor de administración virtual actual y el Servidor de administración principal.
3. Haga clic en el nombre de la cuenta de usuario que desee designar como propietario del dispositivo.

4. En la ventana que se abre con la configuración del usuario, seleccione la pestaña **Dispositivos**.
5. Haga clic en **Agregar**.
6. En la lista de dispositivos, seleccione el dispositivo que desee asignar al usuario.
7. Haga clic en **Aceptar**.

El dispositivo seleccionado se agrega a la lista de dispositivos asignados al usuario.

Como alternativa para realizar esta operación, ingrese a **Activos (dispositivos)** → **Dispositivos administrados**, haga clic en el nombre del dispositivo que desee asignar y luego haga clic en el vínculo **Administrar propietario del dispositivo**.

## Configurar la verificación en dos pasos para todos los usuarios

Este procedimiento describe cómo habilitar la verificación en dos pasos para todos los usuarios y cómo excluir cuentas de usuario de la verificación en dos pasos. Si no habilitó la verificación en dos pasos para su cuenta antes de habilitarla para otros usuarios, la aplicación abre primero la ventana para habilitar la verificación en dos pasos para su cuenta. Este procedimiento también describe cómo habilitar la verificación en dos pasos para su cuenta.

> Si habilitó la verificación en dos pasos para su cuenta, puede pasar a la etapa de habilitación de la verificación en dos pasos para todos los usuarios.

### Requisitos previos

Antes de comenzar:

- Asegúrese de que su cuenta de usuario tenga el derecho de Modificar ACL de objeto del área funcional **Características generales: Permisos de usuario** para modificar la configuración de seguridad de las cuentas de otros usuarios.
- Asegúrese de que los demás usuarios del Servidor de administración instalen una aplicación de autenticación en sus dispositivos.

### Etapas

La habilitación de la verificación en dos pasos para todos los usuarios se realiza en etapas:

1. **Instalar una aplicación de autenticación en un dispositivo**

   Puede usar cualquier aplicación que admita el algoritmo de contraseña de un solo uso basado en el tiempo (TOTP), por ejemplo:

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex ID

- Avanpost Authenticator
- Aladdin 2FA

Para comprobar si Kaspersky Security Center es compatible con la aplicación de autenticación que desea utilizar, habilite la verificación en dos pasos para todos los usuarios o para un usuario en particular.

En uno de los pasos, se sugiere indicar el código de seguridad generado por la aplicación de autenticación. Si tiene éxito, Kaspersky Security Center es compatible con el autenticador seleccionado.

No recomendamos en absoluto instalar la app de autenticación en el mismo dispositivo desde el que se establece la conexión con el Servidor de administración.

2. **Sincronizar la hora de la aplicación de autenticación con la hora del dispositivo en el que está instalado el Servidor de administración**

   Asegúrese de que la hora del dispositivo en el que esté instalada la aplicación de autenticación y la hora del dispositivo que contenga el Servidor de administración estén sincronizadas con UTC a través de fuentes de tiempo externas. De lo contrario, pueden producirse errores durante la autenticación y la activación de la verificación en dos pasos.

3. **Habilitar la verificación en dos pasos para su cuenta y recibir la clave secreta de su cuenta**

   Instrucciones:

   - Para la Consola de administración basada en MMC: habilitación de la verificación en dos pasos para su cuenta
   - Para Kaspersky Security Center Web Console: habilitación de la verificación en dos pasos para su cuenta

   Después de habilitar la verificación en dos pasos para su cuenta, puede habilitar la verificación en dos pasos para todos los usuarios.

4. **Habilitación de la verificación en dos pasos para todos los usuarios**

   Los usuarios con la verificación en dos pasos habilitada deben usarla para iniciar sesión en el Servidor de administración.

   Instrucciones:

   - Para la Consola de administración basada en MMC: habilitación de la verificación en dos pasos para todos los usuarios
   - Para Kaspersky Security Center Web Console: habilitación de la verificación en dos pasos para todos los usuarios

5. **Editar el nombre del emisor de un código de seguridad**

   Si tiene varios Servidores de administración con nombres similares, es posible que tenga que cambiar los nombres de los emisores de códigos de seguridad para que se reconozcan mejor los diferentes Servidores de administración.

   Instrucciones:

   - Para la Consola de administración basada en MMC: editar el nombre del emisor de un código de seguridad
   - Para Kaspersky Security Center Web Console: editar el nombre del emisor de un código de seguridad

6. **Excluir las cuentas de usuario para las que no es necesario habilitar la verificación en dos pasos**

   Si es necesario, puede excluir a los usuarios de la verificación en dos pasos. Los usuarios con cuentas excluidas no tienen que utilizar la verificación en dos pasos para iniciar sesión en el Servidor de administración.

Instrucciones:

- Para la Consola de administración basada en MMC: excluir cuentas de la verificación en dos pasos
- Para Kaspersky Security Center Web Console: excluir cuentas de la verificación en dos pasos

7. **Configuración de la verificación en dos pasos para su cuenta**

   Si los usuarios no están excluidos de la verificación en dos pasos y la verificación en dos pasos aún no se configuró para su cuenta, deben configurarla en la ventana que se abre cuando inician sesión en Kaspersky Security Center. De lo contrario, no podrán acceder al Servidor de administración de acuerdo con sus derechos.

   Instrucciones:

   - Para la Consola de administración basada en MMC: Configuración de la verificación en dos pasos para su cuenta
   - Para Kaspersky Security Center Web Console: Configuración de la verificación en dos pasos para su cuenta

## Resultados

Una vez completado este procedimiento:

- La verificación en dos pasos está habilitada para su cuenta.
- La verificación en dos pasos está habilitada para todas las cuentas de usuario del Servidor de administración, excepto para las cuentas de usuario que fueron excluidas.

## Acerca de la verificación en dos pasos

Cuando la verificación en dos pasos está habilitada para una cuenta, se requiere un código de seguridad de un solo uso, además del nombre de usuario y la contraseña, para iniciar sesión en la Consola de administración o en Kaspersky Security Center Web Console. Con la autenticación de dominio habilitada, el usuario solo necesita ingresar el código de seguridad de un solo uso.

Para usar la verificación en dos pasos, instale en el dispositivo móvil o la computadora una app de autenticación que genere códigos de seguridad de un solo uso. Puede usar cualquier aplicación que admita el algoritmo de contraseña de un solo uso basado en el tiempo (TOTP), por ejemplo:

- Google Authenticator
- Microsoft Authenticator
- Bitrix24 OTP
- Yandex ID
- Avanpost Authenticator
- Aladdin 2FA

Para comprobar si Kaspersky Security Center es compatible con la aplicación de autenticación que desea utilizar, habilite la verificación en dos pasos para todos los usuarios o para un usuario en particular.

En uno de los pasos, se sugiere indicar el código de seguridad generado por la aplicación de autenticación. Si tiene éxito, Kaspersky Security Center es compatible con el autenticador seleccionado.

Recomendamos que guarde la clave secreta o el código QR, y los conserve en un lugar seguro. Con esto podrá restablecer el acceso a Kaspersky Security Center Web Console si no puede utilizar el dispositivo móvil.

Para asegurar el uso de Kaspersky Security Center, puede habilitar la verificación en dos pasos para su cuenta y habilitar la verificación en dos pasos para todos los usuarios.

Puede excluir cuentas de la verificación en dos pasos. Puede ser necesario para las cuentas de servicio que no pueden recibir un código de seguridad para la autenticación.

## Reglas y limitaciones

Para poder activar la verificación en dos pasos para todos los usuarios y desactivar la verificación en dos pasos para usuarios particulares:

- Asegúrese de que su cuenta tenga el derecho Modificar ACL de objeto en el área funcional **Características generales: permisos de usuario**.
- Habilite la verificación en dos pasos para su cuenta.

Para poder desactivar la verificación en dos pasos para todos los usuarios:

- Asegúrese de que su cuenta tenga el derecho Modificar ACL de objeto en el área funcional **Características generales: permisos de usuario**.
- Inicie sesión en Kaspersky Security Center Web Console utilizando la verificación en dos pasos.

Si la verificación en dos pasos está activada para una cuenta de usuario en el Servidor de administración de Kaspersky Security Center versión 13 o posterior, el usuario no podrá conectarse a las versiones 12, 12.1 o 12.2 de Kaspersky Security Center Web Console.

## Volver a emitir la clave secreta

Cualquier usuario puede volver a emitir la clave secreta que se utiliza para la verificación en dos pasos. Cuando un usuario se autentifica con la clave secreta reemitida y la utiliza para iniciar sesión, el Servidor de administración guarda la nueva clave secreta de la cuenta de usuario. Si el usuario ingresa la nueva clave secreta de manera incorrecta, el Servidor de administración no guarda la nueva clave secreta y deja la clave secreta actual válida para la autenticación posterior.

Un código de seguridad tiene un identificador denominado *nombre del emisor*. El nombre del emisor del código de seguridad se utiliza como identificador del Servidor de administración en la aplicación de autenticación. El nombre del emisor del código de seguridad tiene un valor predeterminado que es el mismo que el nombre del Servidor de administración. Puede cambiar el nombre del emisor del código de seguridad. Si cambia el nombre del emisor del código de seguridad, deberá emitir una nueva clave secreta y brindársela a la aplicación de autenticación.

## Habilitación de la verificación en dos pasos para su cuenta (Web Console)

Puede habilitar la verificación en dos pasos solo para su cuenta.

Antes de habilitar la verificación en dos pasos para su cuenta, verifique que haya una app de autenticación instalada en el dispositivo móvil. Asegúrese de que la hora establecida en la aplicación de autenticación esté sincronizada con la hora establecida en el dispositivo en el que está instalado el Servidor de administración.

*Para habilitar la verificación en dos pasos para una cuenta de usuario, siga estos pasos:*

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios**.
2. Haga clic en el nombre de su cuenta.
3. En la ventana que se abre con los ajustes del usuario, seleccione la pestaña **Seguridad de autenticación**.
4. En la pestaña **Seguridad de autenticación**:
   a. Seleccione la opción **Solicitar nombre de usuario, contraseña y código de seguridad (verificación en dos pasos)**. Haga clic en el botón **Guardar**.
   b. En la ventana de verificación de dos pasos que se abre, haga clic en **Cómo configurar la verificación en dos pasos**.
      Ingrese la clave secreta en la app de autenticación instalada en el dispositivo móvil (o, como alternativa, haga clic en **Ver código QR** y, en la app de autenticación, escanee el código QR). Obtendrá un código de seguridad de un solo uso.
   c. En la ventana de verificación en dos pasos, ingrese el código de seguridad generado por la aplicación de autenticación y haga clic en el botón **Confirmar y aplicar**.
5. Haga clic en el botón **Guardar**.

La verificación en dos pasos está habilitada para su cuenta.

## Habilitar la verificación en dos pasos para su cuenta (basada en MMC)

Antes de habilitar la verificación en dos pasos para su cuenta, verifique que haya una app de autenticación instalada en el dispositivo móvil. Asegúrese de que la hora establecida en la app de autenticación esté sincronizada con la hora del Servidor de administración.

*Para habilitar la verificación en dos pasos para su cuenta, siga estos pasos:*

1. En el árbol de la consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y luego seleccione **Propiedades**.
2. En la ventana de propiedades del Servidor de administración, vaya al panel **Secciones** y seleccione **Avanzado** y, a continuación, **Verificación en dos pasos**.

3. En la sección **Verificación en dos pasos**, haga clic en el botón **Configurar**.

   > Si ya habilitó la verificación en dos pasos para la cuenta, al hacer clic en el botón **Configurar**, se restablece la clave secreta para que pueda volver a configurar la verificación en dos pasos.

   En la ventana de propiedades de verificación en dos pasos que se abre, aparecerá la clave secreta.

4. Introduzca la clave secreta en la app de autenticación para recibir el código de seguridad por única vez. Puede especificar manualmente la clave secreta en la app de autenticación o escanear el código QR con la app de autenticación del dispositivo móvil.

5. Especifique el código de seguridad generado por la app de autenticación y haga clic en el botón **Aceptar** para salir de la ventana de propiedades de la verificación en dos pasos.

6. Haga clic en el botón **Aplicar**.

7. Haga clic en el botón **Aceptar**.

La verificación en dos pasos está habilitada para su propia cuenta.

## Habilitar la verificación en dos pasos obligatoria para todos los usuarios (Web Console)

Puede habilitar la verificación en dos pasos para todos los usuarios del Servidor de administración si su cuenta tiene el derecho Modificar ACL de objeto en el área funcional **Características generales: Permisos de usuario** y si es autenticado mediante el uso de la verificación en dos pasos.

*Para habilitar la verificación en dos pasos para todos los usuarios, siga estos pasos:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Seguridad de autenticación** de la ventana de propiedades, cambie el botón de activación de la opción **verificación en dos pasos para todos los usuarios** a la posición de habilitado.

3. Si no habilitó la verificación en dos pasos para su cuenta antes de habilitarla para todos los usuarios, la aplicación abre la ventana para habilitar la verificación en dos pasos para su cuenta.

   a. En la ventana de verificación en dos pasos, haga clic en **Cómo configurar la verificación en dos pasos**.

   b. Ingrese la clave secreta en la aplicación de autenticación o haga clic en **Ver código QR** y escanee el código QR con la aplicación de autenticador en su dispositivo móvil para recibir un código de seguridad de un solo uso.

   c. En la ventana de verificación en dos pasos, especifique el código de seguridad generado por la aplicación de autenticación y, a continuación, haga clic en el botón **Confirmar y aplicar**.

La verificación en dos pasos está habilitada para todos los usuarios. A partir de ahora, los usuarios del Servidor de administración, incluidos los usuarios que se agregaron después de habilitar la verificación en dos pasos para todos los usuarios, tienen que configurar la verificación en dos pasos para sus cuentas, excepto los usuarios que están excluidos de la verificación en dos pasos.

## Habilitar la verificación en dos pasos para todos los usuarios (basada en MMC)

Puede habilitar la verificación en dos pasos para todos los usuarios del Servidor de administración si su cuenta tiene el derecho Modificar ACL de objeto en el área funcional **Características generales: Permisos de usuario** y si es autenticado mediante el uso de la verificación en dos pasos.

*Para habilitar la verificación en dos pasos para todos los usuarios, siga estos pasos:*

1. En el árbol de la consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y luego seleccione **Propiedades**.
2. En la ventana de propiedades del Servidor de administración, en el panel **Secciones**, seleccione **Avanzado** y, a continuación, **Verificación en dos pasos**.
3. Haga clic en el botón **Obligatoria para todos** para habilitar la verificación en dos pasos para todos los usuarios.
4. Si no habilitó la verificación en dos pasos para su cuenta antes de habilitarla para todos los usuarios, la aplicación abre la ventana para habilitar la verificación en dos pasos para su cuenta.
   a. Ingrese la clave secreta en la app de autenticación para recibir el código de seguridad de un solo uso. Puede especificar la clave secreta manualmente en la app de autenticación o escanear el código QR con la app de autenticación del dispositivo móvil para recibir un código de seguridad de un solo uso.
   b. Especifique el código de seguridad generado por la app de autenticación y haga clic en el botón **Aceptar** para salir de la ventana de propiedades de la verificación en dos pasos.
5. En la sección **Verificación en dos pasos**, haga clic en el botón **Aplicar** y, a continuación, en el botón **Aceptar**.

La verificación en dos pasos está habilitada para todos los usuarios. A partir de ahora, todos los usuarios del Servidor de administración, incluidos los usuarios que se agregaron después de habilitar esta opción, tienen que configurar la verificación en dos pasos para sus cuentas, excepto los usuarios cuyas cuentas están excluidas de la verificación en dos pasos.

## Deshabilitar la verificación en dos pasos para una cuenta de usuario (Web Console)

Puede deshabilitar la verificación en dos pasos para su cuenta, así como para una cuenta de cualquier otro usuario.

Puede deshabilitar la verificación en dos pasos de la cuenta de otro usuario si su cuenta tiene el derecho Modificar ACL de objeto en el área funcional **Características generales: permisos de usuario** y si se autentica su acceso mediante el uso de la verificación en dos pasos.

*Para deshabilitar la verificación en dos pasos para una cuenta de usuario, siga estos pasos:*

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios**.
2. Haga doble clic en la cuenta de usuario interna para la que desea deshabilitar la verificación en dos pasos. Puede ser su propia cuenta o la de cualquier otro usuario.
3. En la ventana que se abre con los ajustes del usuario, seleccione la pestaña **Protección de cuentas**.

4. En la pestaña **Protección de cuentas**, seleccione la opción **Solo solicitar nombre de usuario y contraseña** si desea deshabilitar la verificación en dos pasos para una cuenta de usuario.

5. Haga clic en el botón **Guardar**.

La verificación en dos pasos está deshabilitada para la cuenta de usuario.

Si desea restaurar el acceso de un usuario que no puede iniciar sesión en Kaspersky Security Center Web Console mediante la verificación en dos pasos, deshabilite la verificación en esta cuenta de usuario y luego seleccione la opción **Solo solicitar nombre de usuario y contraseña** como se describe anteriormente. Después, inicie sesión en Kaspersky Security Center Web Console con la cuenta de usuario para la cual deshabilitó la verificación en dos pasos y vuelva a habilitarla.

## Deshabilitar la verificación en dos pasos para una cuenta de usuario (basada en MMC)

*Para deshabilitar la verificación en dos pasos para su propia cuenta, siga estos pasos:*

1. En el árbol de la consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y luego seleccione **Propiedades**.

2. En la ventana de propiedades del Servidor de administración, en el panel **Secciones**, seleccione **Avanzado** y, a continuación, **Verificación en dos pasos**.

3. En la sección **Verificación en dos pasos**, haga clic en el botón **Desactivar**.

4. Haga clic en el botón **Aplicar**.

5. Haga clic en el botón **Aceptar**.

La verificación en dos pasos está inhabilitada para su cuenta.

Puede deshabilitar la verificación en dos pasos de las cuentas de otros usuarios. Esto brinda protección en caso de que, por ejemplo, un usuario pierda o rompa un dispositivo móvil.

Puede deshabilitar la verificación en dos pasos de la cuenta de otro usuario solo si tiene el derecho Modificar ACL de objeto en el área funcional **Características generales: permisos de usuario** y si se autentica su acceso mediante el uso de la verificación en dos pasos. Siguiendo los pasos a continuación, también puede deshabilitar la verificación en dos pasos para su propia cuenta.

*Para deshabilitar la verificación en dos pasos para cualquier cuenta de usuario, siga estos pasos:*

1. En el árbol de consola, abra la carpeta **Cuentas de usuario**.

   De manera predeterminada, la carpeta **Cuentas de usuario** es una subcarpeta de la carpeta **Avanzado**.

2. En el espacio de trabajo, haga doble clic en la cuenta de usuario para la que desea deshabilitar la verificación en dos pasos.

   Para todas las cuentas de usuario para las que está habilitada la verificación en dos pasos, la columna **2FA obligatoria** se establece en **Sí**.

3. En la ventana de **Propiedades:<user name>** que se abre, seleccione la sección **Verificación en dos pasos**.

4. En la sección **Verificación en dos pasos**, seleccione las siguientes opciones:

   - Si desea deshabilitar la verificación en dos pasos para una cuenta de usuario, haga clic en el botón **Deshabilitar**.

   - Si desea excluir esta cuenta de usuario de la verificación en dos pasos, seleccione la opción **El usuario podrá autenticarse con solo ingresar su nombre de usuario y contraseña**.

5. Haga clic en el botón **Aplicar**.

6. Haga clic en el botón **Aceptar**.

La verificación en dos pasos para una cuenta de usuario está deshabilitada.

Si desea restaurar el acceso de un usuario que no puede iniciar sesión en la Consola de administración mediante la verificación en dos pasos, deshabilite la verificación en dos pasos para la cuenta de este usuario y seleccione la opción **El usuario podrá autenticarse con solo ingresar su nombre de usuario y contraseña** en **Verificación en dos pasos** como se describe arriba. Después, inicie sesión en la Consola de administración con la cuenta de usuario para la cual deshabilitó la verificación en dos pasos y vuelva a habilitarla.

## Deshabilitar la verificación en dos pasos obligatoria para todos los usuarios (Web Console)

Puede deshabilitar la verificación en dos pasos obligatoria para todos los usuarios si la verificación en dos pasos está habilitada para su cuenta y su cuenta tiene el derecho Modificar ACL de objeto en el área funcional **Características generales: permisos de usuario**. Si la verificación en dos pasos está deshabilitada para su cuenta, debe habilitar la verificación en dos pasos para su cuenta antes de deshabilitarla para todos los usuarios.

*Para deshabilitar la verificación en dos pasos para todos los usuarios, siga estos pasos:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Seguridad de autenticación** de la ventana de propiedades, cambie el botón de activación de la opción **verificación en dos pasos para todos los usuarios** a la posición de deshabilitado.

La verificación en dos pasos está inhabilitada para todos los usuarios. La deshabilitación de la verificación en dos pasos para todos los usuarios no se aplica a las cuentas específicas para las que la verificación en dos pasos se había habilitado antes por separado.

## Deshabilitar la verificación en dos pasos obligatoria para todos los usuarios (basada en MMC)

Puede deshabilitar la verificación en dos pasos obligatoria para todos los usuarios del Servidor de administración si tiene el derecho Modificar ACL de objeto en el área funcional **Características generales: permisos de usuario** y si se autentica su acceso mediante la verificación en dos pasos.

*Para deshabilitar la verificación en dos pasos para todos los usuarios, siga estos pasos:*

1. En el árbol de la consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y luego seleccione **Propiedades**.
2. En la ventana de propiedades del Servidor de administración, en el panel **Secciones**, seleccione **Avanzado** y, a continuación, **Verificación en dos pasos**.
3. Haga clic en el botón **Opcional para todos** para deshabilitar la verificación en dos pasos para todos los usuarios.
4. Haga clic en el botón **Aplicar** en la sección **Verificación en dos pasos**.
5. Haga clic en el botón **Aceptar** en la sección **Verificación en dos pasos**.

La verificación en dos pasos está inhabilitada para todos los usuarios. La deshabilitación de la verificación en dos pasos para todos los usuarios no se aplica a las cuentas específicas para las que la verificación en dos pasos se había habilitado antes por separado.

## Excluir cuentas de la verificación en dos pasos (Web Console)

Puede excluir las cuentas de usuario de la verificación en dos pasos si tiene el derecho Modificar ACL de objeto en el área funcional **Características generales: Permisos de usuario**.

Si una cuenta de usuario se excluye de la lista de verificación en dos pasos para todos los usuarios, este usuario no tiene que utilizar la verificación en dos pasos.

> Puede ser necesario excluir cuentas de la verificación en dos pasos para las cuentas de servicio que no pueden pasar el código de seguridad durante la autenticación.

*Si quiere excluir algunas cuentas de usuario de la verificación en dos pasos:*

1. Debe realizar un sondeo del controlador de dominio de Active Directory de Microsoft para actualizar la lista de usuarios del Servidor de administración si desea excluir una cuenta de Active Directory.
2. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.
3. En la pestaña **Seguridad de autenticación** de la ventana de propiedades, en la tabla de exclusiones de la verificación en dos pasos haga clic en el botón **Agregar**.
4. En la ventana que se abre:
   a. Seleccione las cuentas de usuario que desea excluir.
   b. Haga clic en el botón **Aceptar**.

Las cuentas de usuario seleccionadas se excluyen de la verificación en dos pasos.

## Excluir cuentas de la verificación en dos pasos (basada en MMC)

Puede excluir una cuenta de la verificación en dos pasos si su cuenta tiene el derecho Modificar ACL de objeto en el área funcional **Características generales: Permisos de usuario**.

Si una cuenta de usuario está excluida de la verificación en dos pasos, dicho usuario puede iniciar sesión en la Consola de administración o en Kaspersky Security Center Web Console sin utilizar la verificación en dos pasos.

Puede ser necesario excluir cuentas de la verificación en dos pasos para las cuentas de servicio que no pueden pasar el código de seguridad durante la autenticación.

*Para excluir una cuenta de usuario de la verificación en dos pasos:*

1. Si desea excluir una cuenta de Active Directory, realice un sondeo de Active Directory para actualizar la lista de usuarios del Servidor de administración.
2. En el árbol de consola, abra la carpeta **Cuentas de usuario**.

   De manera predeterminada, la carpeta **Cuentas de usuario** es una subcarpeta de la carpeta **Avanzado**.
3. En el espacio de trabajo, haga doble clic en la cuenta de usuario que desea excluir de la verificación en dos pasos.
4. En la ventana de **Propiedades:<user name>** que se abre, seleccione la sección **Verificación en dos pasos**.
5. En la sección abierta, seleccione la opción **El usuario podrá autenticarse con solo ingresar su nombre de usuario y contraseña**.
6. En la sección **Verificación en dos pasos**, haga clic en el botón **Aplicar** y, a continuación, en el botón **Aceptar**.

Esta cuenta de usuario se excluye de la verificación en dos pasos. Puede comprobar las cuentas excluidas en la lista de cuentas de usuario.

## Editar el nombre del emisor de un código de seguridad (Web Console)

Puede tener varios identificadores (se denominan emisores) para diferentes Servidores de administración. Puede cambiar el nombre del emisor de un código de seguridad en caso de que, por ejemplo, el Servidor de administración ya utilice un nombre similar de emisor del código de seguridad para otro Servidor de administración. De forma predeterminada, el nombre del emisor de un código de seguridad es el mismo que el nombre del Servidor de administración.

Tras cambiar el nombre del emisor del código de seguridad, debe reemitir una nueva clave secreta y brindársela a la aplicación de autenticación.

*Para especificar un nuevo nombre de emisor del código de seguridad, siga estos pasos:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la ventana que se abre con los ajustes del usuario, seleccione la pestaña **Protección de cuentas**.

3. En la pestaña **Protección de cuentas**, haga clic en el vínculo **Editar**.

   Se abre la sección **Editar el emisor del código de seguridad**.

4. Se especifica un nuevo nombre de emisor del código de seguridad.

5. Haga clic en el botón **Aceptar**.

Se especifica un nuevo nombre de emisor del código de seguridad para el Servidor de administración.

## Editar el nombre del emisor de un código de seguridad (basada en MMC)

Puede tener varios identificadores (se denominan emisores) para diferentes Servidores de administración. Puede cambiar el nombre del emisor de un código de seguridad en caso de que, por ejemplo, el Servidor de administración ya utilice un nombre similar de emisor del código de seguridad para otro Servidor de administración. De forma predeterminada, el nombre del emisor de un código de seguridad es el mismo que el nombre del Servidor de administración.

Tras cambiar el nombre del emisor del código de seguridad, debe reemitir una nueva clave secreta y brindársela a la aplicación de autenticación.

*Para especificar un nuevo nombre de emisor de un código de seguridad, siga estos pasos:*

1. En el árbol de la consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y luego seleccione **Propiedades**.

2. En la ventana de propiedades del Servidor de administración, en el panel **Secciones**, seleccione **Avanzado** y, a continuación, **Verificación en dos pasos**.

3. Especifique un nuevo nombre de emisor de código de seguridad en el campo **Emisor del código de seguridad**.

4. Haga clic en el botón **Aplicar** en la sección **Verificación en dos pasos**.

5. Haga clic en el botón **Aceptar** en la sección **Verificación en dos pasos**.

Se especifica un nuevo nombre de emisor del código de seguridad para el Servidor de administración.

## Configurar la verificación en dos pasos para su cuenta (Web Console)

La primera vez que inicia sesión en Kaspersky Security Center después de habilitar la verificación en dos pasos, se abre la ventana para configurar la verificación en dos pasos para su propia cuenta.

Antes de configurar la verificación en dos pasos para su cuenta, verifique que haya una app de autenticación instalada en el dispositivo móvil.

Asegúrese de que la hora del dispositivo en el que esté instalada la aplicación de autenticación y la hora del dispositivo que contenga el Servidor de administración estén sincronizadas con UTC a través de fuentes de tiempo externas.

*Para configurar la verificación en dos pasos para su cuenta, siga estos pasos:*

1. Genere un código de seguridad de un solo uso mediante la app de autenticación en el dispositivo móvil. Para ello, realice una de las siguientes acciones:

   - Ingrese manualmente la clave secreta en la aplicación de autenticación.
   - Haga clic en **Ver código QR** y escanee el código QR con la aplicación de autenticación.

   Aparecerá un código de seguridad en el dispositivo móvil.

2. En la ventana para configurar la verificación en dos pasos, ingrese el código de seguridad generado por la aplicación de autenticación y haga clic en el botón **Confirmar y aplicar**.

La verificación en dos pasos se configura para su cuenta. Puede acceder al Servidor de administración de acuerdo con sus derechos.

## Configurar la verificación en dos pasos para su cuenta (basada en MMC)

La primera vez que inicia sesión en Kaspersky Security Center después de habilitar la verificación en dos pasos, se abre la ventana para configurar la verificación en dos pasos para su propia cuenta.

Antes de configurar la verificación en dos pasos para su cuenta, verifique que haya una app de autenticación instalada en el dispositivo móvil. Asegúrese de que la hora del dispositivo en el que esté instalada la aplicación de autenticación y la hora del dispositivo que contenga el Servidor de administración estén sincronizadas con UTC a través de fuentes de tiempo externas.

*Para configurar la verificación en dos pasos para su cuenta, siga estos pasos:*

1. Genere un código de seguridad de un solo uso mediante la app de autenticación en el dispositivo móvil. Para ello, realice una de las siguientes acciones:

   - Ingrese manualmente la clave secreta en la aplicación de autenticación.
   - Escanee el código QR mediante la app de autenticación.

   Aparecerá un código de seguridad en el dispositivo móvil.

2. En la ventana **Habilitar la verificación en dos pasos**, especifique el código de seguridad generado por la app de autenticación y, a continuación, haga clic en el botón **Aceptar**.

La verificación en dos pasos se configura para su cuenta. Puede acceder al Servidor de administración de acuerdo con sus derechos.

## Generar una nueva clave secreta

Puede generar una nueva clave secreta para una verificación en dos pasos para su cuenta solo si está autorizado a utilizar la verificación en dos pasos.

*Para generar una nueva clave secreta para una cuenta de usuario, siga los siguientes pasos:*

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios**.
2. Haga clic en el nombre de la cuenta de usuario para la que desea generar una nueva clave secreta para la verificación en dos pasos.
3. En la ventana que se abre con los ajustes del usuario, seleccione la pestaña **Protección de cuentas**.
4. En la pestaña **Protección de cuentas**, haga clic en el vínculo **Generar una clave secreta nueva**.
5. En la ventana de verificación en dos pasos que se abre, ingrese una nueva clave de seguridad generada por la aplicación de autenticación.
6. Haga clic en el botón **Confirmar y aplicar**.

Se genera una nueva clave secreta para el usuario.

Si pierde el dispositivo móvil, puede instalar una app de autenticación en otro dispositivo móvil y generar una nueva clave secreta para restaurar el acceso a Kaspersky Security Center Web Console.

## Prohibir a los nuevos usuarios configurar la verificación en dos pasos por sí mismos

Para mejorar aún más la seguridad del acceso a Kaspersky Security Center Web Console, puede prohibir a los nuevos usuarios configurar ellos mismos la verificación en dos pasos.

Si esta opción está habilitada, un usuario con la verificación en dos pasos deshabilitada, por ejemplo, un nuevo administrador de dominio, no puede configurar la verificación en dos pasos por sí mismo. Por lo tanto, dicho usuario no puede autenticarse en el Servidor de administración y no puede iniciar sesión en Kaspersky Security Center Web Console sin la aprobación de otro administrador de Kaspersky Security Center que ya tenga activada la verificación en dos pasos.

Esta opción está disponible si la verificación en dos pasos está habilitada para todos los usuarios.

*Para prohibir a los nuevos usuarios configurar la verificación en dos pasos por sí mismos:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Seguridad de autenticación** de la ventana de propiedades, cambie la posición del interruptor **Prohibir a los nuevos usuarios configurar la verificación en dos pasos por sí mismos** a la posición habilitada.

Esta opción no afecta las cuentas de usuario agregadas a las exclusiones de verificación en dos pasos.

Para otorgar acceso a Kaspersky Security Center Web Console a un usuario con la verificación en dos pasos deshabilitada, desactive temporalmente la opción **Prohibir a los nuevos usuarios configurar la verificación en dos pasos por sí mismos**, solicite al usuario que habilite la verificación en dos pasos y luego active la opción de regreso.

## Asignar a un usuario como propietario del dispositivo tras instalar el Agente de red

*Para permitir que el usuario se registre como propietario de un dispositivo Linux:*

1. En Kaspersky Security Center Web Console, vaya a **Descubrimiento y despliegue** → **Despliegue y asignación** → **Paquetes de instalación**.

   Se abrirá la lista de paquetes de instalación.

2. Haga clic en el paquete de instalación del Agente de red.

   Se abrirá la ventana de propiedades del paquete de instalación.

3. En la ventana de propiedades del paquete de instalación, haga clic en **Configuración** → **Avanzado**.

4. En la sección **Registro de usuario como propietario de un dispositivo (solo Linux)**, active la opción **Permitir la ejecución de la utilidad de registro de usuario luego de la instalación del Agente de red** y haga clic en **Guardar**.

La utilidad para registrar al usuario como propietario del dispositivo se puede ejecutar a través de la línea de comandos en el dispositivo cliente.

*Para registrar un usuario como propietario de un dispositivo Linux en el dispositivo cliente:*

1. Ejecute el siguiente comando en la línea de comandos en el dispositivo cliente:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner
   ```

2. Ingrese el nombre de usuario y la contraseña, si se le solicitan estos datos.

   Si el nombre de usuario y la contraseña están incluidos en el archivo de respuesta o en el paquete de instalación del Agente de red, ejecute el siguiente comando en la línea de comando del dispositivo cliente:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended
   ```

Si el usuario forma parte de un grupo de seguridad interno, el nombre de usuario debe ser el mismo.

Si el usuario forma parte de un grupo de seguridad de Active Directory, el nombre de usuario debe constar del nombre de usuario y el nombre de dominio.

Si la verificación en dos pasos está activada para el usuario, debe ingresar la contraseña temporal de un solo uso (TOTP) de la aplicación.

Se registrará al usuario como propietario del dispositivo.

## Eliminar un usuario o un grupo de seguridad

Solo puede eliminar usuarios internos o grupos de seguridad internos.

*Para eliminar un usuario o un grupo de seguridad:*

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos**, y luego seleccione la pestaña **Usuarios** o **Grupos**.
2. Seleccione la casilla de verificación junto al usuario o el grupo de seguridad que desea eliminar.
3. Haga clic en **Eliminar**.
4. En la ventana que se abre, haga clic en **Aceptar**.

Se elimina el usuario o el grupo de seguridad.

## Cambiar la contraseña de una cuenta de usuario

Es posible que deba cambiar la contraseña de su propia cuenta o de otra cuenta de usuario si la contraseña vigente está a punto de caducar o si desea cambiarla por otra más segura.

La contraseña debe cumplir con las siguientes reglas:

- La contraseña debe tener entre 8 y 256 caracteres.
- La contraseña debe incluir caracteres de al menos tres de los grupos enumerados a continuación:
  - Letras mayúsculas (A-Z)
  - Letras minúsculas (a-z)
  - Números (0-9)
  - Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- La contraseña no debe contener espacios en blanco, caracteres Unicode o la combinación de "." y "@" cuando "." está colocado delante de "@".

## Cambiar la contraseña de la cuenta propia

*Pasos para cambiar la contraseña de su propia cuenta:*

1. En el menú principal, vaya a la configuración de su cuenta y seleccione **Cambiar contraseña**.
2. Ingrese la contraseña actual y especifique la nueva contraseña para la conexión a Kaspersky Security Center.

   Para ver la contraseña ingresada, haga clic en .
3. Si su cuenta está protegida contra modificaciones no autorizadas, verifique si tiene los permisos necesarios para modificarla. En la ventana **Protección de cuentas**, ingrese las credenciales de su cuenta o de una cuenta que tenga el derecho Modificar ACL de objeto en el área funcional Características generales: Permisos de usuario.
4. Si la verificación en dos pasos está habilitada para la cuenta que utilizó en el paso anterior, ingrese el código de seguridad que generó la app de autenticación en el dispositivo móvil.

## Cambiar la contraseña de una cuenta de usuario interno

*Pasos para cambiar la contraseña de una cuenta de usuario interna:*

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
2. Haga clic en el nombre de la cuenta de usuario que desee editar.
3. En la ventana de configuración de usuario que se abre, en la pestaña **General**, haga clic en el botón **Cambiar contraseña**.
4. Establezca una contraseña nueva para la conexión del usuario a Kaspersky Security Center.

   Para ver la contraseña ingresada, haga clic en .
5. Si es necesario, active la opción **El usuario debe cambiar la contraseña la primera vez que inicie sesión** para forzar el cambio de contraseña la siguiente vez que el usuario se autentique.
6. Si la cuenta de usuario está protegida contra modificaciones no autorizadas, verifique si tiene los permisos necesarios para modificarla. En la ventana **Protección de cuentas**, ingrese las credenciales de una cuenta que tenga el derecho Modificar ACL de objeto en el área funcional Características generales: Permisos de usuario.

### Configurar las opciones para cambiar la contraseña mediante indicadores de servidor

Puede usar la utilidad klscflag y los siguientes comandos para configurar el cambio de contraseñas:

- Configuración del período de rotación de contraseñas (indicador `LP_SplPwdChangePeriodDays`)

  `klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <período_de_rotación>`

  Dónde `<período_de_rotación>` es un período de tiempo en días después del cual expira la contraseña del usuario. Valores posibles: 0-730. Si el valor del parámetro es 0, la rotación de contraseñas queda deshabilitada.

- Configuración del tiempo de la advertencia preliminar sobre la necesidad de cambiar la contraseña (el indicador `LP_SplPwdChangeNotificationHours`)

  `klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <tiempo_de_advertencia>`

  Dónde `<tiempo_de_advertencia>` es un período de tiempo en horas antes de que expire la contraseña del usuario. Durante este número de horas, se mostrará una notificación para indicar que se necesita un cambio de clave. Valores posibles: 0-17520. Si el valor del parámetro es 0, el tiempo de advertencia será un 25 por ciento del período de rotación de contraseñas.

- Configuración del valor predeterminado de la opción **El usuario debe cambiar la contraseña la primera vez que inicie sesión** (indicador `LP_SplPwdForceChange`)

  `klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v <valor>`

  Donde los posibles valores del indicador `<valor>`:

  `1`: la opción **El usuario debe cambiar la contraseña la primera vez que inicie sesión** está habilitada.

  `0`: la opción **El usuario debe cambiar la contraseña la primera vez que inicie sesión** está deshabilitada.

Para ver el valor vigente de un indicador, ejecute el siguiente comando:

`klscflag.exe -fget -pv .core/.independent -s KLLIM -n <indicador> -t d`

La variable `<indicador>` debe ser `LP_SplPwdChangePeriodDays`, `LP_SplPwdChangeNotificationHours` o `LP_SplPwdForceChange`.

## Creación de roles de usuario

*Para crear un rol de usuario:*

1. En el menú principal, vaya a **Usuarios y roles** → **Roles**.
2. Haga clic en **Agregar**.
3. En la ventana **Nombre del nuevo rol** que se abre, introduzca el nombre del nuevo rol.
4. Haga clic en **Aceptar** para aplicar los cambios.

5. Cuando se abra la ventana de propiedades del rol, cambie la configuración del rol:

   - En la pestaña **General**, modifique el nombre del rol.

     No es posible modificar el nombre de los roles predefinidos.

   - En la pestaña **Configuración**, modifique el alcance del rol, así como las directivas y los perfiles asociados al rol.

   - En la pestaña **Derechos de acceso**, modifique los derechos de acceso a las aplicaciones de Kaspersky.

6. Haga clic en **Guardar** para guardar los cambios.

El nuevo rol aparece en la lista de roles de usuario.

## Editar un rol de usuario

*Para editar un rol de usuario:*

1. En el menú principal, vaya a **Usuarios y roles** → **Roles**.

2. Haga clic en el nombre del rol que desee editar.

3. Cuando se abra la ventana de propiedades del rol, cambie la configuración del rol:

   - En la pestaña **General**, modifique el nombre del rol.

     No es posible modificar el nombre de los roles predefinidos.

   - En la pestaña **Configuración**, modifique el alcance del rol, así como las directivas y los perfiles asociados al rol.

   - En la pestaña **Derechos de acceso**, modifique los derechos de acceso a las aplicaciones de Kaspersky.

4. Haga clic en **Guardar** para guardar los cambios.

El rol actualizado aparece en la lista de roles de usuario.

## Editar el alcance de un rol de usuario

El *alcance de un rol de usuario* es una combinación de usuarios y grupos de administración. Los ajustes asociados a un rol de usuario se aplican únicamente a los dispositivos que pertenecen a los usuarios que tienen ese rol, y solo cuando esos dispositivos pertenecen a grupos y subgrupos asociados al rol en cuestión.

*Para agregar usuarios, grupos de seguridad y grupos de administración al alcance de un rol de usuario, puede utilizar cualquiera de los siguientes métodos:*

*Método 1:*

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos**, y luego seleccione la pestaña **Usuarios** o **Grupos**.

2. Active las casillas de verificación ubicadas junto a los usuarios y grupos de seguridad que desee agregar al alcance del rol de usuario.

3. Haga clic en el botón **Asignar rol**.

   Se inicia el asistente de asignación de roles. Avance por el asistente utilizando el botón **Siguiente**.

4. En el paso **Seleccionar rol**, seleccione el rol de usuario que desee asignar.

5. En el paso **Definir alcance**, seleccione el grupo de administración que desee agregar al alcance del rol de usuario.

6. Haga clic en el botón **Asignar rol** para cerrar la ventana.

Los usuarios o grupos de seguridad y el grupo de administración seleccionados se agregan al alcance del rol de usuario.

*Método 2:*

1. En el menú principal, vaya a **Usuarios y roles** → **Roles**.

2. Haga clic en el nombre del rol cuyo alcance desee definir.

3. Cuando se abra la ventana de propiedades del rol, seleccione la pestaña **Configuración**.

4. En la sección **Alcance del rol**, haga clic en **Agregar**.

   Se inicia el asistente de asignación de roles. Avance por el asistente utilizando el botón **Siguiente**.

5. En el paso **Definir alcance**, seleccione el grupo de administración que desee agregar al alcance del rol de usuario.

6. En el paso **Seleccionar usuarios**, seleccione los usuarios y los grupos de seguridad que desee agregar al alcance del rol de usuario.

7. Haga clic en el botón **Asignar rol** para cerrar la ventana.

8. Haga clic en el botón **Cerrar** (⨯) para cerrar la ventana de propiedades del rol.

Los usuarios o grupos de seguridad y el grupo de administración seleccionados se agregan al alcance del rol de usuario.

*Método 3:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Derechos de acceso**, seleccione la casilla de verificación junto al nombre del usuario o del grupo de seguridad que desee agregar al alcance de un rol de usuario y, luego, haga clic en el botón **Roles**.

   No puede seleccionar varios usuarios o grupos de seguridad al mismo tiempo. Si selecciona más de un elemento, el botón **Roles** se deshabilitará.

3. En la ventana **Roles**, seleccione el rol de usuario que desee asignar, aplíquelo y guarde los cambios.

   Los usuarios o grupos de seguridad seleccionados se agregan al alcance del rol de usuario.

## Eliminar un rol de usuario

*Para eliminar un rol de usuario:*

1. En el menú principal, vaya a **Usuarios y roles** → **Roles**.
2. Marque la casilla ubicada junto al nombre del rol que desee eliminar.
3. Haga clic en **Eliminar**.
4. En la ventana que se abre, haga clic en **Aceptar**.

Se elimina el rol de usuario.

## Asociación de perfiles de directivas con roles

Los roles de usuario pueden asociarse a perfiles de directivas. Al crear una asociación entre un perfil de directiva y un rol, la regla de activación del perfil pasa a depender del rol y, en consecuencia, el perfil de directiva se activa para los usuarios que tienen el rol especificado.

A modo de ejemplo, suponga que los dispositivos de un grupo de administración, llamado Usuarios, están sujetos a una directiva que prohíbe el uso de aplicaciones de navegación GPS. Existe un solo dispositivo en el grupo que necesita contar con un navegador GPS: el dispositivo que le pertenece al mensajero. En esta situación, puede asignar un rol llamado "Mensajero" al propietario de este dispositivo y crear un perfil de directiva que permita utilizar aplicaciones de navegación GPS solo en aquellos dispositivos que pertenezcan a usuarios con el rol "Mensajero". Los demás ajustes de la directiva se mantendrán sin cambios. Solo el usuario que tenga el rol "Mensajero" podrá ejecutar el software de navegación GPS. Si posteriormente se le asigna el rol "Mensajero" a otro empleado más, esa persona también podrá ejecutar aplicaciones de navegación en el dispositivo que le provea la organización. El software de navegación GPS seguirá estando prohibido en los demás dispositivos del grupo de administración.

*Para asociar un rol con un perfil de directiva:*

1. En el menú principal, vaya a **Usuarios y roles** → **Roles**.
2. Haga clic en el nombre del rol que desee asociar con un perfil de directiva.

   Se abre la ventana de propiedades del rol, con la pestaña **General** seleccionada.

3. Seleccione la pestaña **Configuración** y desplácese hacia abajo hasta llegar a la sección **Directivas y perfiles**.

4. Haga clic en **Editar**.

5. Asocie el rol con un perfil de directiva nuevo o existente:

   - Para asociar el rol con **un perfil de directiva existente**, haga clic en el corchete angular (>) ubicado junto al nombre de la directiva pertinente, busque el nombre del perfil con el que quiera asociar el rol y active la casilla adyacente a ese perfil.

   - Para asociar el rol con **un nuevo perfil de directiva**:

     a. Marque la casilla adyacente a la directiva para la que se vaya a crear el perfil.

     b. Haga clic en **Nuevo perfil de directiva**.

     c. Escriba el nombre del nuevo perfil y configure sus opciones.

     d. Haga clic en el botón **Guardar**.

     e. Marque la casilla adyacente al nuevo perfil.

6. Haga clic en **Asignar a rol**.

El perfil quedará asociado al rol y aparecerá en las propiedades del rol. El perfil se aplicará automáticamente al dispositivo de toda persona que tenga asignado el rol.

## Propagación de roles de usuario a Servidores de administración secundarios

De forma predeterminada, las listas de funciones del usuario de los Servidores de administración principal y secundario son independientes. Puede configurar la aplicación para propagar automáticamente las funciones de usuario creadas en el Servidor de administración principal a todos los Servidores de administración secundarios. Las funciones de usuario también pueden propagarse desde un Servidor de administración secundario a sus propios Servidores de administración secundarios.

*Para propagar funciones de usuario desde el Servidor de administración principal a los Servidores de administración secundarios:*

1. En el menú principal, haga clic en el icono de configuración (  ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abrirá la ventana de propiedades del Servidor de administración, con la pestaña **General** seleccionada.

2. Vaya a la sección **Jerarquía de Servidores de administración**.

3. Habilite la opción **Propagar la lista de roles a los Servidores de administración secundarios** y, luego, haga clic en el botón **Guardar**.

La aplicación copia las funciones de usuario del Servidor de administración principal a los Servidores de administración secundarios.

Cuando la opción **Propagar la lista de roles a los Servidores de administración secundarios** está habilitada, y las funciones de usuario se propagan, no se pueden editar ni eliminar en los Servidores de administración secundarios. Cuando crea una nueva función o edita una existente en el Servidor de administración principal, los cambios se copian automáticamente en los Servidores de administración secundarios. Cuando elimina una función de usuario en el Servidor de administración principal, esta función permanece en los Servidores de administración secundarios posteriormente, pero se puede editar o eliminar.

Las funciones que se propagan al Servidor de administración secundario desde el Servidor principal se muestran con la marca de verificación verde (✓). No puede modificar estas funciones en el Servidor de administración secundario.

Si crea una función en el Servidor de administración principal y hay una función con el mismo nombre en su Servidor de administración secundarios, el nuevo rol se copia al Servidor de administración secundario con el índice agregado a su nombre, por ejemplo, ~~ 1, ~~ 2 (el índice puede ser aleatorio).

Si deshabilita la opción **Propagar la lista de roles a los Servidores de administración secundarios**, todas las funciones de usuario permanecen en los Servidores de administración secundarios, pero se vuelven independientes de las del Servidor de administración principal. Después de volverse independientes, las funciones de usuario de los Servidores de administración secundarios se pueden editar o eliminar.

## Cambiar la contraseña de una cuenta

Puede cambiar la contraseña de una cuenta local si, por ejemplo, el usuario olvida la contraseña de su cuenta local o si debe realizarse un cambio de contraseña programado.

El cambio de contraseña se aplicará incluso si el usuario no ha iniciado sesión con su cuenta. También puede cambiarse la contraseña de la cuenta root local.

> Esta tarea solo se puede realizar en dispositivos Linux.

*Para cambiar la contraseña de la cuenta local en dispositivos específicos:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea.
3. En el campo **Tipo de tarea**, seleccione **Cambiar contraseña de la cuenta (solo Linux)**.

4. Seleccione una de las siguientes opciones:

- **Asignar tarea a un grupo de administración**

  La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

  Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

  Si la tarea se asigna a un grupo de administración, la pestaña **Seguridad** no se mostrará en la ventana de propiedades de la tarea; esto se debe a que las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

- **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**

  Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

  Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.

- **Asignar tarea a una selección de dispositivos**

  La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

  Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

La tarea *Cambiar contraseña de la cuenta (solo Linux)* se creará para los dispositivos especificados. Si seleccionó la opción **Asignar tarea a un grupo de administración**, la tarea será una tarea de grupo.

5. En el paso **Alcance de la tarea**, indique un grupo de administración, dispositivos con direcciones específicas o una selección de dispositivos.

   Los ajustes disponibles dependerán de la opción seleccionada en el paso anterior.

6. En el paso **Ingresar nombre de la cuenta y contraseña nueva**, defina los siguientes ajustes:

   - En el campo **Nombre de cuenta**, ingrese el nombre de la cuenta cuya contraseña desee cambiar.
   - En el campo **Nueva contraseña**, ingrese la contraseña que se establecerá para la cuenta indicada en el campo anterior.

     Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.
   - Si es necesario, marque la casilla **Establecer como contraseña de un solo uso (el usuario debe cambiar la contraseña después del primer inicio de sesión)**.

     - Establecer como contraseña de un solo uso (el usuario debe cambiar la contraseña después del primer inicio de sesión)

       Si se marca esta casilla, se le pedirá al usuario que establezca una nueva contraseña después del primer inicio de sesión.

       Si no se marca esta casilla, no se le pedirá al usuario que establezca una nueva contraseña después del primer inicio de sesión.

       Esta casilla no está marcada de manera predeterminada.

7. En el paso **Finalizar la creación de la tarea**, haga clic en el botón **Finalizar** para crear la tarea y cerrar el asistente.

   Si habilitó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abrirá la ventana de configuración de la tarea. Utilice esta ventana para, de ser necesario, revisar y modificar los ajustes de la tarea o programar su ejecución.

8. En la lista de tareas, seleccione la tarea creada y haga clic en **Iniciar**.

   Como alternativa, puede esperar a que ocurra el inicio programado definido en los ajustes de la tarea.

Cuando finaliza la tarea de cambio de contraseña, se cambia la contraseña de la cuenta local indicada en los dispositivos especificados.

Para garantizar el correcto funcionamiento de las tareas de cambio de contraseña, debe deshabilitarse SELinux en el dispositivo del usuario.

## Revocar los derechos de administrador local

Puede revocar los derechos de administrador local de las cuentas. Ello brinda una capa de control adicional sobre las cuentas de usuario. Los derechos de administrador local pueden revocarse, por ejemplo, una vez que finaliza un encargo puntual.

Cuando se ejecuta esta tarea, se verifica si la cuenta local indicada pertenece a grupos de administradores locales. Estos grupos se definen en la configuración de la directiva del Agente de red. Puede personalizar la lista de grupos de administradores locales en la configuración de la directiva del Agente de red. También puede ver la lista de cuentas de usuarios con privilegios especiales en el **Informe sobre usuarios privilegiados en el dispositivo (solo Linux)**.

Esta tarea solo se puede realizar en dispositivos Linux.

*Para revocar los derechos de administrador local en dispositivos específicos:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea.
3. En el campo **Tipo de tarea**, seleccione **Revocar derechos de administrador local (solo Linux)**.
4. Seleccione una de las siguientes opciones:

   - Asignar tarea a un grupo de administración

     La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

     Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

     Si la tarea se asigna a un grupo de administración, la pestaña **Seguridad** no se mostrará en la ventana de propiedades de la tarea; esto se debe a que las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

   - Especificar las direcciones de los dispositivos manualmente o importarlas de una lista

     Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

     Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.

   - Asignar tarea a una selección de dispositivos

     La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

     Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

   La tarea *Revocar derechos de administrador local (solo Linux)* se creará para los dispositivos indicados. Si seleccionó la opción **Asignar tarea a un grupo de administración**, la tarea será una tarea de grupo.
5. En el paso **Alcance de la tarea**, indique un grupo de administración, dispositivos con direcciones específicas o una selección de dispositivos.

   Los ajustes disponibles dependerán de la opción seleccionada en el paso anterior.

6. En este paso del asistente, defina los siguientes ajustes:

   - En el grupo **Modo operativo**, seleccione un modo de funcionamiento:

     - **Revocar derechos de administrador local de las cuentas enumeradas**

       Si selecciona esta opción, se revocarán los derechos de administrador local de las cuentas locales indicadas.

       Esta opción está seleccionada de forma predeterminada.

     - **Excluir cuentas enumeradas de la revocación de derechos de administrador local**

       Si selecciona esta opción, se revocarán los derechos de administrador local de todas las cuentas locales, excepto las enumeradas.

       Esta opción no está seleccionada de manera predeterminada.

   - Indique las cuentas locales:

     - Haga clic en **Agregar**.

     - En la ventana que se abre, haga lo siguiente:

       - En el campo **Nombre de cuenta**, ingrese el nombre de la cuenta local.

       - En el grupo de opciones **Acción de la cuenta** (disponible solo si se ha seleccionado la opción **Revocar derechos de administrador local de las cuentas enumeradas**, seleccione la acción.

       - **Conservar cuenta**

         Si selecciona esta opción, la cuenta local no se eliminará después de que se revoquen los derechos de administrador local.

         Esta opción está seleccionada de forma predeterminada.

       - **Eliminar cuenta**

         Si selecciona esta opción, la cuenta local se eliminará independientemente de si tiene derechos de administrador local.

         Esta opción no está seleccionada de manera predeterminada.

7. En el paso **Finalizar la creación de la tarea**, haga clic en el botón **Finalizar** para crear la tarea y cerrar el asistente.

   Si habilitó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abrirá la ventana de configuración de la tarea. Utilice esta ventana para, de ser necesario, revisar y modificar los ajustes de la tarea o programar su ejecución.

8. En la lista de tareas, seleccione la tarea creada y haga clic en **Iniciar**.

   Como alternativa, puede esperar a que ocurra el inicio programado definido en los ajustes de la tarea.

Cuando se complete la tarea de revocación de derechos de administrador local, se revocarán los derechos de administrador local de las cuentas locales indicadas en los dispositivos seleccionados.

# Administración de revisiones de objetos

En esta sección encontrará información sobre la administración de revisiones de objetos. Kaspersky Security Center permite que usted siga la modificación de objeto. Cuando un objeto se modifica de algún modo, se crea una *revisión*. Cada revisión lleva un número que la identifica.

Los objetos de aplicación que admiten la administración de la revisión incluyen:

- Propiedades del Servidor de administración
- Directivas
- Tareas
- Grupos de administración
- Cuentas de usuario
- Paquetes de instalación

Puede realizar las siguientes acciones con las revisiones de los objetos:

- Ver una revisión seleccionada (disponible solo para directivas)
- Revertir los cambios realizados en un objeto a una revisión seleccionada
- Guardar revisiones como archivo JSON (disponible solo para directivas)

Todo objeto compatible con la administración de revisiones tiene una sección llamada **Historial de revisiones** en su ventana de propiedades. La sección contiene una lista de revisiones asociadas al objeto y los siguientes datos:

- **Revisión** número de revisión del objeto.
- **Hora** fecha y hora de modificación del objeto.
- **Usuario** nombre del usuario que modificó el objeto.
- **Dirección IP del dispositivo del usuario** dirección IP del dispositivo desde el que se modificó el objeto.
- **Dirección IP de Web Console** dirección IP de Kaspersky Security Center Web Console con la que se modificó el objeto.
- **Acción** acción realizada en el objeto.
- **Descripción** descripción de la revisión vinculada al cambio en la configuración del objeto.

  De forma predeterminada, la descripción de las revisiones está en blanco. Para agregar una descripción a una revisión, seleccione la revisión pertinente y haga clic en el botón **Editar descripción**. En la ventana abierta, ingrese un texto que describa la revisión.

## Devolver un objeto a una revisión anterior

Los cambios realizados en un objeto pueden revertirse. Por ejemplo, puede volver a dejar la configuración de una directiva tal como estaba en una fecha puntual.

*Para revertir los cambios realizados en un objeto:*

1. En la ventana de propiedades del objeto, abra la pestaña **Historial de revisiones**.
2. En la lista de revisiones de objeto, seleccione la revisión a la que quiere revertir los cambios.
3. Haga clic en el botón **Revertir**.
4. Haga clic en **Aceptar** para confirmar la operación.

   El objeto volverá a la revisión seleccionada. La lista de revisiones del objeto mostrará un registro de la acción que se tomó. En la descripción de la revisión, verá especificado el número de revisión a la que haya regresado el objeto.

La operación de revertir los cambios solo está disponible para objetos de directiva y tareas.

## Agregar una descripción a una revisión

Kaspersky Security Center permite que usted siga la modificación de objeto. Cuando un objeto se modifica de algún modo, se crea una revisión. Cada revisión lleva un número que la identifica.

Para ayudarse a encontrar una revisión específica en la lista, puede agregarle una descripción.

*Para agregar una descripción a una revisión:*

1. En la ventana de propiedades del objeto, abra la pestaña **Historial de revisiones**.
2. En la lista de revisiones del objeto, seleccione la revisión a la que desea agregar la descripción.
3. Haga clic en el botón **Editar descripción**.

   Se abre la ventana **Descripción**.
4. En la ventana **Descripción**, ingrese un texto que describa la revisión.

   De forma predeterminada, la descripción de las revisiones está en blanco.
5. Guarde la descripción de la revisión.

Se agrega la descripción a la revisión del objeto.

## Ver y guardar una revisión de una directiva

Kaspersky Security Center le permite ver qué modificaciones se realizaron en una directiva durante un período determinado, así como guardar información sobre estas modificaciones en un archivo.

Para que pueda ver y guardar la revisión de una directiva, el complemento web de administración correspondiente debe ofrecerle esta prestación.

*Para ver una revisión de una directiva:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en la directiva a la que corresponda la revisión que desee ver y vaya a la sección **Historial de revisiones**.
3. En la lista de revisiones de la directiva, haga clic en el número de revisión que desee ver.

   Si el tamaño de una revisión es superior a 10 MB, no podrá verla mediante Kaspersky Security Center Web Console. Se le pedirá que guarde la revisión seleccionada en un archivo JSON.

   Si el tamaño de la revisión no supera los 10 MB, se mostrará un informe en formato HTML con la configuración de la revisión de directiva seleccionada. Dado que el informe se muestra en una ventana emergente, asegúrese de que las ventanas emergentes estén permitidas en su navegador.

*Para guardar la revisión de una directiva en un archivo JSON:*

En la lista de revisiones de la directiva, seleccione la revisión que desee guardar y luego haga clic en **Guardar en archivo**.

La revisión se guardará en un archivo JSON.

# Eliminación de objetos

Esta sección proporciona información sobre cómo eliminar objetos.

Puede eliminar objetos como los siguientes:

- Directivas
- Tareas
- Paquetes de instalación
- Servidores de administración virtuales
- Usuarios
- Grupos de seguridad
- Grupos de administración

*Para eliminar un objeto:*

1. Abra la sección correspondiente de Kaspersky Security Center Web Console y luego seleccione el objeto.
2. En la barra de herramientas, haga clic en el botón **Eliminar**.
3. En la ventana que se abre, haga clic en **Aceptar** para confirmar su selección.

Se elimina el objeto seleccionado.

Cuando se elimina un objeto, se conserva información sobre el mismo en la base de datos. El plazo de almacenamiento para la información sobre los objetos eliminados es el mismo que el plazo de almacenamiento para las revisiones de objetos (el plazo recomendado es de 90 días). Puede cambiar el plazo de almacenamiento solo si tiene el permiso **Modificar** en el área de derechos **Objetos eliminados**.

## Acercad de la eliminación de dispositivos cliente

Cuando elimina un dispositivo administrado de un grupo de administración, la aplicación mueve el dispositivo al grupo de Dispositivos no asignados. Después de eliminar el dispositivo, las aplicaciones de Kaspersky instaladas (Agente de red y cualquier aplicación de seguridad, por ejemplo, Kaspersky Endpoint Security) permanecen en el dispositivo.

Kaspersky Security Center maneja los dispositivos del grupo Dispositivos no asignados según las siguientes reglas:

- Si configuró reglas de movimiento de dispositivos y un dispositivo cumple con los criterios de una regla de movimiento, el dispositivo se mueve automáticamente a un grupo de administración de acuerdo con la regla.
- El dispositivo se almacena en el grupo de Dispositivos no asignados y se elimina automáticamente del grupo de acuerdo con las reglas de retención de dispositivos.

  Las reglas de retención de dispositivos no afectan a los dispositivos que tienen una o más unidades cifradas con cifrado de disco completo. Dichos dispositivos no se eliminan automáticamente, solo puede hacerlo de forma manual. Si necesita eliminar un dispositivo con una unidad cifrada, primero descifre la unidad y, luego, elimine el dispositivo.

  > Cuando elimina un dispositivo que tiene una unidad cifrada, también se eliminan los datos necesarios para descifrar la unidad. Si selecciona la casilla **Comprendo el riesgo y deseo eliminar los dispositivos seleccionados** en la ventana de confirmación que se abre cuando elimina dichos dispositivos (ya sea del grupo **Dispositivos no asignados** o **Dispositivos administrados**), significa que está al tanto de la subsecuente eliminación de datos.

  Para descifrar la unidad, se deben cumplir las siguientes condiciones:

  - El dispositivo se vuelve a conectar al Servidor de administración para restaurar los datos necesarios para descifrar la unidad.
  - El usuario del dispositivo recuerda la contraseña de descifrado.
  - La aplicación de seguridad que se usó para cifrar la unidad, por ejemplo, Kaspersky Endpoint Security para Windows, todavía está instalada en el dispositivo.

  Si la tecnología Kaspersky Disk Encryption descifró la unidad, también puede intentar recuperar los datos con la utilidad de restauración FDERT.

> En VDI, si tiene un dispositivo con unidades cifradas, la información de la unidad cifrada se elimina después de eliminar el dispositivo.

Cuando elimina manualmente un dispositivo del grupo de Dispositivos no asignados, la aplicación elimina el dispositivo de la lista. Después de eliminar el dispositivo, las aplicaciones de Kaspersky instaladas (si las hay) permanecen en el dispositivo. Después, si el dispositivo sigue estando visible para el Servidor de administración y ha configurado un sondeo de red regular, Kaspersky Security Center detecta el dispositivo durante el sondeo de red y lo agrega nuevamente al grupo Dispositivos no asignados. Por lo tanto, es razonable eliminar un dispositivo manualmente solo si el servidor de administración no puede ver el dispositivo.

# Kaspersky Security Network (KSN)

En esta sección se describe cómo usar la infraestructura de servicios en línea llamada Kaspersky Security Network (KSN). Aquí encontrará información detallada sobre KSN e instrucciones para habilitar KSN, configurar el acceso a KSN y ver las estadísticas de uso del servidor proxy de KSN.

> Es posible que la funcionalidad de las actualizaciones (incluida la provisión de actualizaciones de firmas antivirus y actualizaciones de base de código) y la funcionalidad de KSN no estén disponibles en el software en los EE. UU.

# Acerca de KSN

Kaspersky Security Network (KSN) es una infraestructura de servicios en línea que brinda acceso a la base de conocimientos en línea de Kaspersky, que contiene información sobre la reputación de los archivos, los recursos web y el software. El uso de los datos de Kaspersky Security Network garantiza una respuesta más rápida de las aplicaciones de Kaspersky ante las amenazas, mejora la eficacia de algunos componentes de protección y reduce el riesgo de falsos positivos. KSN permite utilizar las bases de datos de reputación de Kaspersky para obtener información sobre las aplicaciones instaladas en los dispositivos administrados.

Kaspersky Security Center es compatible con las siguientes soluciones de infraestructura:

- *KSN*. Esta solución permite intercambiar información con Kaspersky Security Network. Al participar en KSN, acepta enviar a Kaspersky, de manera automática, información sobre el funcionamiento de las aplicaciones de Kaspersky instaladas en los dispositivos cliente que se administran mediante Kaspersky Security Center. La información se transfiere de conformidad con la configuración de acceso a KSN. Los analistas de Kaspersky realizan un examen adicional de la información recibida y la suman a las bases de datos de estadísticas y de reputación de Kaspersky Security Network. Kaspersky Security Center utiliza esta solución de forma predeterminada.

- *Kaspersky Private Security Network (KPSN)* es una solución que permite a los usuarios de dispositivos con aplicaciones de Kaspersky instaladas obtener acceso a bases de datos de reputación de Kaspersky Security Network y otros datos estadísticos, sin enviar datos a KSN Global desde sus propios dispositivos. KPSN diseñada para clientes corporativos que, por alguno de los siguientes motivos, no pueden participar en Kaspersky Security Network:

  - Los dispositivos de los usuarios no tienen acceso a Internet.

  - La transmisión de datos fuera del país o de la LAN corporativa está prohibida por ley o por las directivas de seguridad corporativas.

  Puede configurar los ajustes de acceso de Kaspersky Private Security Network en la sección **Configuración del proxy de KSN** de la ventana de propiedades del Servidor de administración.

La aplicación le preguntará si desea unirse a KSN cuando ejecute el Asistente de inicio rápido. Puede iniciar o detener el uso de KSN en cualquier momento cuando use la aplicación.

Utiliza KSN de acuerdo con la Declaración de KSN que lee y acepta cuando habilita KSN. Si se actualiza la Declaración de KSN, se le mostrará cuando actualice una versión del Servidor de administración. Puede aceptar la Declaración de KSN actualizada o rechazarla. Si la rechaza, seguirá usando KSN de acuerdo con la versión anterior de la Declaración de KSN que aceptó anteriormente.

Cuando KSN está habilitado, Kaspersky Security Center comprueba que haya acceso a los servidores de KSN. Si los servidores DNS configurados en el sistema no permiten acceder a los servidores de Kaspersky, la aplicación utiliza servidores DNS públicos. Esto se hace para garantizar que los dispositivos administrados no vean afectado su nivel de seguridad.

Los dispositivos cliente administrados por el Servidor de administración interactúan con KSN mediante el servidor proxy de KSN. El servidor proxy de KSN proporciona las funciones siguientes:

- Permite que los dispositivos cliente envíen solicitudes a KSN, obtengan información de KSN y transfieran información a KSN, incluso cuando no tengan acceso directo a Internet.

- El servidor proxy de KSN almacena en caché los datos procesados y reduce, de esta manera, la carga en el canal de salida y el período de tiempo que se utiliza para esperar información solicitada por un dispositivo cliente.

Puede configurar el servidor proxy de KSN en la sección **Configuración del proxy de KSN** de la ventana de propiedades del Servidor de administración.

## Configurar el acceso a KSN

Puede configurar el acceso a Kaspersky Security Network (KSN) en el Servidor de administración y en un punto de distribución.

*Para configurar el acceso del Servidor de administración a KSN:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Configuración del proxy de KSN**.

3. Cambie el botón de activación a la posición **Habilitar el proxy de KSN en el Servidor de administración Habilitado**.

   Si esta opción está habilitada, el servidor proxy de KSN envía datos a KSN para aumentar la eficiencia de los componentes de Kaspersky Security Center y mejorar el rendimiento de las aplicaciones de Kaspersky. Los datos se envían desde los dispositivos cliente a KSN de acuerdo con la directiva de Kaspersky Endpoint Security activa en esos dispositivos. Si se deshabilita el interruptor, no se enviarán datos a KSN desde el Servidor de administración y los dispositivos cliente a través de Kaspersky Security Center. Sin embargo, los dispositivos cliente podrán enviar datos directamente a KSN (es decir, sin pasar por Kaspersky Security Center), según lo determine su configuración. La directiva de Kaspersky Endpoint Security, que está activa en los dispositivos cliente, determina qué datos se enviarán de los dispositivos a KSN en forma directa (es decir, sin pasar por Kaspersky Security Center).

4. Cambie el interruptor a la posición **Usar Kaspersky Security Network Habilitado**.

   Si se habilita esta opción, los dispositivos cliente enviarán los resultados de instalación de parches a Kaspersky. Al activar esta opción, asegúrese de leer y aceptar los términos de la Declaración de KSN.

   Si está utilizando KPSN, cambie el botón interruptor a la posición **Usar Kaspersky Private Security Network Habilitado** y haga clic en el botón **Seleccionar archivo de configuración del proxy de KSN** para descargar la configuración de KPSN Privada (archivos con las extensiones pkcs7 y pem). Una vez descargada la configuración, la interfaz muestra el nombre y contactos del proveedor, así como la fecha de creación del archivo con la configuración de KPSN.

   > Cuando habilite KPSN, preste atención a los puntos de distribución configurados para enviar solicitudes de KSN directamente a Cloud KSN. Los puntos de distribución que tengan instalado el Agente de red versión 11 (o versiones anteriores) continuarán enviando solicitudes KSN a Cloud KSN. Para reconfigurar los puntos de distribución a fin de enviar solicitudes de KSN a KPSN, habilite la opción **Transmitir las solicitudes para KSN al Servidor de administración** para cada punto de distribución. Puede habilitar esta opción en las propiedades del punto de distribución o en la directiva del Agente de red.

   Cuando cambie el botón interruptor a la posición **Usar Kaspersky Private Security Network Habilitado**, aparecerá un mensaje con los detalles sobre KPSN.

   Las siguientes aplicaciones de Kaspersky son compatibles con KPSN:

   - Kaspersky Security Center
   - Kaspersky Endpoint Security para Windows
   - Kaspersky Endpoint Security for Linux
   - Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2
   - Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

   Si habilita KPSN en Kaspersky Security Center, se les comunicará a estas aplicaciones que el servicio utilizado es KPSN. En la ventana de configuración de la aplicación, en la subsección de **Kaspersky Security Network** de la sección **Protección avanzada contra amenazas**, se muestra la información sobre el proveedor KSN seleccionado: KSN o KPSN.

   > Si usa versiones de la aplicación anteriores a Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 o anterior a Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent al ejecutar KPSN, recomendamos que use Servidores de administración secundarios para los cuales el uso de KPSN no esté habilitado.

   > Kaspersky Security Center no envía ningún dato estadístico a Kaspersky Security Network si se configura KPSN en la sección **Configuración del proxy de KSN** de la ventana de propiedades del Servidor de administración.

5. Si tiene las configuraciones del servidor proxy configuradas en las propiedades del Servidor de administración, pero su arquitectura de red requiere que use KPSN directamente, habilite la opción **No usar el servidor proxy configurado para conectarse a KPSN**. De lo contrario, las solicitudes de las aplicaciones administradas no podrán llegar a KPSN.

6. Configure la conexión del Servidor de administración al servicio del proxy de KSN:

   - En **Configuración de la conexión**, en el campo **Puerto TCP**, ingrese el número del puerto TCP que se utilizará para conectarse al servidor proxy de KSN. El puerto predeterminado para conectarse al servidor proxy de KSN es el 13111.

   - Si desea que el Servidor de administración se conecte al servidor proxy de KSN a través de un puerto UDP, habilite la opción **Usar puerto UDP** e ingrese el número de puerto en el campo **Puerto UDP**. Esta opción está desactivada de forma predeterminada y se utiliza el puerto TCP. Si habilita esta opción, de forma predeterminada, se usará el puerto UDP 15111 para establecer conexión con el servidor proxy de KSN.

   - Si desea que el Servidor de administración se conecte al servidor proxy de KSN a través de un puerto HTTPS, habilite la opción **Usar HTTPS** y especifique un número de puerto para **HTTPS a través de este puerto**. Esta opción está desactivada de forma predeterminada y se utiliza el puerto TCP. Si habilita esta opción, el puerto HTTPS predeterminado de conexión al servidor proxy de KSN es 17111.

7. Cambie el botón de alternancia a la posición **Conectar los servidores de administración secundarios a KSN por medio del Servidor de administración principal Habilitado**.

   Cuando esta opción está habilitada, los servidores de administración secundarios utilizan el Servidor de administración principal como servidor proxy de KSN. Si esta opción está desactivada, los Servidores de administración secundarios se conectan a KSN por sus propios medios. En este caso, los dispositivos administrados usan Servidores de administración secundarios como servidores proxy de KSN.

   > Los Servidores de administración secundarios usan el Servidor de administración principal como un servidor proxy si en el panel derecho de la sección **Configuración del proxy de KSN**, en las propiedades de los Servidores de administración secundarios, se cambia el botón de habilitación a la posición **Habilitar el proxy de KSN en el Servidor de administración Habilitado**.

8. Haga clic en el botón **Guardar**.

Se guardará la configuración de acceso a KSN.

También puede configurar el acceso de puntos de distribución a KSN, por ejemplo, si desea reducir la carga en el Servidor de administración. El punto de distribución que actúa como un servidor proxy KSN envía solicitudes de KSN desde dispositivos administrados a Kaspersky directamente, sin utilizar el Servidor de administración.

*Para configurar el acceso del punto de distribución a Kaspersky Security Network (KSN):*

1. Asegúrese de que el punto de distribución se asigne manualmente.

2. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

3. En la pestaña **General**, elija la sección **Puntos de distribución**.

4. Haga clic en el nombre del punto de distribución para abrir la ventana de propiedades.

5. En la ventana de propiedades del punto de distribución, en la sección **Proxy de KSN**, habilite la opción **Habilitar el proxy de KSN en el lado del punto de distribución** y, a continuación, habilite la opción **Acceder a KSN Cloud/KPSN directamente a través de Internet**.

6. Haga clic en **Aceptar**.

El punto de distribución actuará como servidor proxy de KSN.

## Habilitar y deshabilitar el uso de KSN

*Pasos para habilitar el uso de KSN:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Configuración del proxy de KSN**.

3. Cambie el botón de activación a la posición **Habilitar el proxy de KSN en el Servidor de administración Habilitado**.

El servidor proxy de KSN está activado y envía datos a KSN para aumentar la eficiencia de los componentes de Kaspersky Security Center y mejorar el rendimiento de las aplicaciones de Kaspersky.

1. Dependiendo de la solución de infraestructura de KSN que utiliza, habilite los botones interruptores correspondientes.

   - Si utiliza KSN Global, cambie el botón interruptor a la posición **Usar Kaspersky Security Network Habilitado**.

     Ya está disponible el envío de datos a KSN. Al activar esta opción, asegúrese de leer y aceptar las condiciones de la Declaración de KSN.

   - Si está usando KPSN, cambie el botón de alternancia a **Usar Kaspersky Private Security Network Habilitado** posición y, a continuación, haga clic en el botón **Seleccionar archivo de configuración del proxy de KSN** para descargar la configuración de KPSN (archivos con las extensiones pkcs7 y pem). Una vez descargada la configuración, la interfaz muestra el nombre y contactos del proveedor, así como la fecha de creación del archivo con la configuración de KPSN.

     Cuando cambie el botón interruptor a la posición **Usar Kaspersky Private Security Network Habilitado**, aparecerá un mensaje con los detalles sobre KPSN.

2. Haga clic en el botón **Guardar**.

*Pasos para deshabilitar el uso de KSN:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Configuración del proxy de KSN**.

3. Cambie el botón interruptor a la posición **Habilitar el proxy de KSN en el Servidor de administración Deshabilitado** para deshabilitar el servicio del proxy de KSN.

4. Haga clic en el botón **Guardar**.

# Ver la Declaración de KSN aceptada

Para habilitar Kaspersky Security Network (KSN), debe leer y aceptar la Declaración de KSN. Si ya ha aceptado la Declaración de KSN y quiere verla nuevamente, puede hacerlo en cualquier momento.

*Para ver la Declaración de KSN aceptada:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Configuración del proxy de KSN**.

3. Haga clic en el enlace **Ver la Declaración de Kaspersky Security Network**.

En la ventana que se abre, puede ver el texto de la Declaración de KSN aceptada.

# Aceptar una Declaración de KSN actualizada

Utiliza KSN de acuerdo con la Declaración de KSN que lee y acepta cuando habilita KSN. Si se actualiza la Declaración de KSN, se le mostrará cuando actualice una versión del Servidor de administración. Puede aceptar la Declaración de KSN actualizada o rechazarla. Si la rechaza, seguirá usando KSN bajo los términos estipulados en la versión que ya haya aceptado de la Declaración de KSN.

Después de actualizar una versión del Servidor de administración, la Declaración de KSN actualizada se muestra automáticamente. Si rechaza la Declaración de KSN actualizada, de todos modos podrá verla y aceptarla más adelante.

*Para ver y luego aceptar o rechazar una Declaración de KSN actualizada:*

1. Haga clic en el vínculo **Ver notificaciones** en la esquina superior derecha de la ventana principal de la aplicación.

   Se abre la ventana **Notificaciones**.

2. Haga clic en el enlace **Ver la Declaración de KSN actualizada**.

   Se abre la ventana **Actualización de la Declaración de Kaspersky Security Network**.

3. Lea la Declaración de KSN y haga clic en el botón que responda a su decisión:

   - **Acepto la Declaración de KSN actualizada**
   - **Utilizar KSN con la antigua Declaración**

Según su elección, KSN sigue funcionando de acuerdo con los términos de la Declaración de KSN actual o actualizada. Puede ver el texto de la Declaración de KSN aceptada en las propiedades del Servidor de administración en cualquier momento.

## Verificar si el punto de distribución opera como servidor proxy de KSN

Puede habilitar un servidor proxy de KSN en un dispositivo administrado asignado para funcionar como punto de distribución. Para funcionar como proxy de KSN, el dispositivo administrado debe tener activo el servicio ksnproxy. Puede verificar, activar o desactivar este servicio en el dispositivo localmente.

El dispositivo designado como punto de distribución puede utilizar Windows o Linux. El modo de llevar a cabo la verificación en el punto de distribución depende del sistema operativo instalado en el punto de distribución.

*Para comprobar si el punto de distribución basado en Windows está operando como servidor proxy de KSN:*

1. En el dispositivo de punto de distribución, en Windows, abra **Servicios** (**Todos los programas** → **Herramientas administrativas** → **Servicios**).

2. En la lista de servicios, verifique si el servicio ksnproxy se está ejecutando.

   Si el servicio ksnproxy se está ejecutando, entonces el Agente de red del dispositivo participa en Kaspersky Security Network y funciona como servidor proxy de KSN para los dispositivos administrados incluidos en el alcance del punto de distribución.

Si lo desea, puede desactivar el servicio ksnproxy. En este caso, el Agente de red del punto de distribución deja de participar en Kaspersky Security Network. Esto requiere derechos de administrador local.

*Para verificar si un punto de distribución con Linux opera como servidor proxy de KSN:*

1. En el dispositivo que actúe como punto de distribución, abra la lista de procesos en ejecución.

2. En la lista de procesos en ejecución, compruebe si[[/opt/kaspersky/ksc64/sbin/ksnproxy]] el proceso se está ejecutando.

Si el servicio ksnproxy se está ejecutando, entonces el Agente de red del dispositivo participa en Kaspersky Security Network y funciona como servidor proxy de KSN para los dispositivos administrados incluidos en el alcance del punto de distribución.

# Escenario de actualización de Kaspersky Security Center y aplicaciones de seguridad administradas

En esta sección se describe el breve escenario principal que puede seguir para actualizar Kaspersky Security Center y las aplicaciones de seguridad administradas.

El proceso para actualizar Kaspersky Security Center y las aplicaciones de seguridad administradas se divide en etapas:

1. **Controlar los requisitos de hardware y software**

   Asegúrese de que su hardware cumpla con los requisitos e instale las actualizaciones requeridas.

2. **Planificando los recursos**

   Determine cuánto espacio en disco ocupa su base de datos. Asegúrese de tener suficiente espacio en el disco para almacenar la copia de seguridad de la configuración y la base de datos del Servidor de administración.

3. **Obtención del archivo de instalación para Kaspersky Security Center**

   Obtenga el archivo ejecutable de la versión actual de Kaspersky Security Center y guárdelo en el dispositivo que funcionará como Servidor de administración. Lea las Notas de la publicación de la versión de Kaspersky Security Center que desea usar.

4. **Creando una copia de seguridad de la versión anterior**

   Utilice la utilidad de copia de seguridad y recuperación de datos para crear una copia de seguridad de los datos del Servidor de administración. También puede crear una tarea de copia de seguridad.

   Se recomienda exportar la lista de complementos instalados.

5. **Ejecutando el instalador**

   Ejecute el archivo ejecutable para la última versión de Kaspersky Security Center. Al ejecutar el archivo, especifique que tiene una copia de seguridad y especifique su ubicación. Sus datos serán restaurados desde la copia de seguridad.

6. **Actualización de las aplicaciones administradas**

   Puede actualizar la aplicación si hay una versión disponible más reciente. Lea la lista de aplicaciones admitidas de Kaspersky y asegúrese de que su versión de Kaspersky Security Center sea compatible con esta aplicación. Después, realice la actualización de la aplicación como se describe en sus Notas de publicación.

## Resultados

Una vez que complete las etapas del escenario de actualización, verifique en Microsoft Management Console que la nueva versión del Servidor de administración se haya instalado correctamente. Haga clic en **Ayuda** → **Acerca de Kaspersky Security Center**. Se muestra la versión.

Para verificar en Kaspersky Security Center Web Console que la versión del Servidor de administración sea la más reciente, en la parte superior de la pantalla, haga clic en el ícono de Configuración ( ) junto al nombre del Servidor de administración. En la ventana de propiedades Servidor de administración que se abre, en la pestaña **General**, seleccione la sección **General**. Se muestra la versión.

Si necesita recuperar los datos del Servidor de administración, siga los pasos descritos en el siguiente tema: Copia de seguridad y recuperación de datos en modo interactivo.

Si actualizó una aplicación de seguridad administrada, asegúrese de que esté correctamente instalada en el (los) dispositivo(s) administrado(s). Para más información, consulte la documentación de esta aplicación.

# Actualización de las bases de datos y las aplicaciones de Kaspersky

En esta sección, se describen los pasos que debe completar para actualizar lo siguiente en forma regular:

- Las bases de datos y los módulos de software de Kaspersky
- Las aplicaciones de Kaspersky que se encuentren instaladas, incluidas las aplicaciones de seguridad y los componentes de Kaspersky Security Center

Es posible que la funcionalidad de las actualizaciones (incluida la provisión de actualizaciones de firmas antivirus y actualizaciones de base de código) y la funcionalidad de KSN no estén disponibles en el software en los EE. UU.

# Procedimiento: actualización regular de bases de datos y aplicaciones de Kaspersky

En esta sección, se detalla un escenario para actualizar regularmente las bases de datos, los módulos de software y las aplicaciones de Kaspersky. Una vez que complete el escenario para configurar la protección de la red, deberá mantener la fiabilidad del sistema de protección. Esto garantizará que los servidores de administración y los dispositivos administrados siempre estén protegidos contra virus, ataques de red, ataques de phishing y otras amenazas.

Para que la protección de la red mantenga su eficacia, debe actualizar periódicamente lo siguiente:

- Las bases de datos y los módulos de software de Kaspersky
- Las aplicaciones de Kaspersky que se encuentren instaladas, incluidas las aplicaciones de seguridad y los componentes de Kaspersky Security Center

Al concluir este escenario, tendrá las siguientes certezas:

- Su red está protegida por el software más reciente de Kaspersky, incluidos los componentes de Kaspersky Security Center y las aplicaciones de seguridad.
- Las bases de datos antivirus y otras bases de datos de Kaspersky críticas para la seguridad de la red estarán siempre actualizadas.

## Requisitos previos

Los dispositivos administrados deben tener conexión con el Servidor de administración. Si no tienen conexión, considere actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky de forma manual o directa desde los servidores de actualización de Kaspersky.

El Servidor de administración debe tener conexión a Internet.

Antes de comenzar, compruebe que hizo lo siguiente:

1. Desplegó las aplicaciones de seguridad de Kaspersky en los dispositivos administrados siguiendo las instrucciones del escenario para desplegar aplicaciones de Kaspersky a través de Kaspersky Security Center Web Console.

2. Creó y configuró todas las directivas, perfiles de directivas y tareas que se requieren según el escenario para configurar la protección de red.

3. Asignó una cantidad apropiada de puntos de distribución de acuerdo con la cantidad de dispositivos administrados y la topología de la red.

El proceso para actualizar las bases de datos y las aplicaciones de Kaspersky se divide en etapas:

**1 Elegir un esquema de actualización**

Existen distintos esquemas para instalar las actualizaciones para los componentes de Kaspersky Security Center y las aplicaciones de seguridad. Elija el esquema o varios esquemas que cumplan con los requisitos de su red.

**2 Crear la tarea para descargar actualizaciones en el repositorio del Servidor de administración**

Esta tarea se crea automáticamente con el asistente de inicio rápido de Kaspersky Security Center. Si no ejecutó el asistente, cree la tarea ahora.

Esta tarea se necesita para descargar actualizaciones de los servidores de actualizaciones de Kaspersky y guardarlas en el repositorio del Servidor de administración. También se la requiere para actualizar las bases de datos y los módulos de software de Kaspersky correspondientes a Kaspersky Security Center. Una vez descargadas, las actualizaciones se pueden propagar a los dispositivos administrados.

Si su red tiene puntos de distribución asignados, las actualizaciones se descargan automáticamente desde el repositorio del Servidor de administración a los repositorios de los puntos de distribución. En este caso, los dispositivos administrados incluidos en el alcance de un punto de distribución descargan las actualizaciones desde el repositorio del punto de distribución en lugar del repositorio del Servidor de administración.

Instrucciones:

- Consola de administración: Creación de la tarea para descargar actualizaciones en el repositorio del Servidor de administración
- Kaspersky Security Center Web Console: Creación de la tarea para descargar actualizaciones en el repositorio del Servidor de administración

**3 Crear la tarea para descargar actualizaciones en los repositorios de los puntos de distribución (opcional)**

De forma predeterminada, las actualizaciones se descargan a los puntos de distribución desde el Servidor de administración. Puede configurar Kaspersky Security Center para descargar las actualizaciones a los puntos de distribución directamente desde los servidores de actualización de Kaspersky. Descargar las actualizaciones en los repositorios de los puntos de distribución es preferible cuando el Servidor de administración no tiene acceso a Internet o cuando transmitir datos entre el Servidor de administración y los puntos de distribución es más costoso que transmitir datos entre los puntos de distribución y los servidores de actualizaciones de Kaspersky.

Si hay puntos de distribución asignados en su red y se creó la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*, los puntos de distribución descargarán las actualizaciones de los servidores de actualizaciones de Kaspersky y no del repositorio del Servidor de administración.

Instrucciones:

- Consola de administración: Creación de la tarea para descargar actualizaciones en los repositorios de los puntos de distribución
- Kaspersky Security Center Web Console: Creación de la tarea para descargar actualizaciones en los repositorios de los puntos de distribución

4. **Configurar los puntos de distribución**

   Si su red tiene puntos de distribución asignados, asegúrese de que la opción **Desplegar actualizaciones** esté habilitada en las propiedades de todos los puntos de distribución pertinentes. Si deja esta opción está deshabilitada en un punto de distribución, los dispositivos incluidos en el alcance del mismo obtendrán sus actualizaciones del repositorio del Servidor de administración.

   Si desea que los dispositivos administrados reciban sus actualizaciones solamente de los puntos de distribución, habilite la opción **Distribuir archivos solo a través de los puntos de distribución** en la directiva del Agente de red.

5. **Habilitar la descarga de actualizaciones sin conexión o el uso de archivos diff para optimizar el proceso de actualización (opcional)**

   Puede optimizar el proceso de actualización utilizando el modelo de descarga de actualizaciones sin conexión (habilitado de forma predeterminada) o utilizando archivos diff. Para cada segmento de red, debe elegir cuál de estas dos características habilitar, ya que no pueden funcionar simultáneamente.

   Cuando el modelo de descarga de actualizaciones sin conexión está habilitado, el Agente de red descarga las actualizaciones necesarias en el dispositivo administrado una vez que las actualizaciones se descargan en el repositorio del Servidor de administración, antes de que la aplicación de seguridad solicite las actualizaciones. Esto mejora la fiabilidad del proceso de actualización. Para usar este modelo, habilite la opción **Descargar actualizaciones y bases de datos antivirus del Servidor de administración con anticipación (recomendado)** en la directiva del Agente de red.

   Si no utiliza el modelo de descarga de actualizaciones sin conexión, puede optimizar el tráfico entre el Servidor de administración y los dispositivos administrados mediante el uso de archivos diff. Cuando esta función está habilitada, el Servidor de administración o un punto de distribución descarga archivos diferenciales en lugar de archivos completos de bases de datos o módulos de software de Kaspersky. Un archivo diff describe las diferencias entre dos versiones de un archivo de una base de datos o de un módulo de software. Por lo tanto, un archivo diff ocupa menos espacio que un archivo completo. Esto reduce el tráfico entre el Servidor de administración o los puntos de distribución y los dispositivos administrados. Para usar esta función, habilite la opción **Descargar archivos diff** en las propiedades de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* o *Descargar actualizaciones en los repositorios de los puntos de distribución*.

   Instrucciones:

   - Usar archivos diff para actualizar las bases de datos y los módulos de software de Kaspersky
   - Consola de administración: Habilitación y deshabilitación del modelo de descarga de actualizaciones sin conexión
   - Kaspersky Security Center Web Console: Habilitación y deshabilitación del modelo de descarga de actualizaciones sin conexión

6. **Verificación de las actualizaciones descargadas (opcional)**

   Antes de instalar las actualizaciones descargadas, puede controlarlas con la tarea *Verificación de actualizaciones*. Esta tarea ejecuta de forma secuencial las tareas de actualización de dispositivos y las tareas de análisis antimalware configuradas a través de ajustes definidos para un grupo específico de dispositivos de prueba. Basándose en los resultados de la tarea, el Servidor de administración inicia o bloquea la propagación de las actualizaciones a los dispositivos restantes.

   La tarea *Verificación de actualizaciones* puede ejecutarse como parte de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. En las propiedades de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, habilite la opción **Verificar actualizaciones antes de distribuirlas** en la Consola de administración o la opción **Ejecutar verificación de actualizaciones** en Kaspersky Security Center Web Console.

   Instrucciones:

   - Consola de administración: Verificación de las actualizaciones descargadas

- Kaspersky Security Center Web Console: Verificación de las actualizaciones descargadas

7. **Aprobar y rechazar actualizaciones de software**

   De forma predeterminada, las actualizaciones de software descargadas tienen el estado *Sin definir*. Puede cambiar este estado a *Aprobada* o *Rechazada*. Las actualizaciones aprobadas siempre se instalan. Si una actualización exige revisar y aceptar los términos del Contrato de licencia de usuario final, es necesario aceptar esos términos para proceder con la instalación. Una vez que se aceptan los términos, la actualización se puede propagar a los dispositivos administrados. Las actualizaciones de estado indefinido solo se pueden instalar en el Agente de red y en otros componentes de Kaspersky Security Center si así lo permite la configuración de la directiva del Agente de red. Las actualizaciones a las que se les asigna el estado *Rechazada* no se instalan en los dispositivos. Si previamente se instaló una actualización rechazada para una aplicación de seguridad, Kaspersky Security Center intentará desinstalar la actualización de todos los dispositivos.

   Aprobar y rechazar actualizaciones solo está disponible para el Agente de red y las aplicaciones de Kaspersky administradas instaladas en dispositivos cliente basados en Windows y en Linux. No se admite la actualización sin interrupciones del Servidor de administración, Kaspersky Security Center Web Console y los complementos web de administración.

   Instrucciones:

   - Consola de administración: Aprobar y rechazar actualizaciones de software
   - Kaspersky Security Center Web Console: Aprobar y rechazar actualizaciones de software

8. **Configurar la instalación automática de actualizaciones y parches para los componentes de Kaspersky Security Center**

   Las actualizaciones y los parches que se descargan para el Agente de red y para los demás componentes de Kaspersky Security Center se instalan automáticamente. Si deja habilitada la opción **Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes** en las propiedades del Agente de red, se instalarán todas las actualizaciones que se descarguen en el repositorio (o en los repositorios). Si deshabilita esta opción, los parches de Kaspersky que se descarguen y que tengan el estado *Sin definir* se instalarán únicamente si cambia su estado a *Aprobada*.

   Instrucciones:

   - Consola de administración: Habilitar y deshabilitar la actualización automática y la aplicación de parches para los componentes de Kaspersky Security Center
   - Kaspersky Security Center Web Console: Habilitar y deshabilitar la actualización automática y la aplicación de parches para los componentes de Kaspersky Security Center

9. **Instalación de actualizaciones para el Servidor de administración**

   Las actualizaciones de software para el Servidor de administración no dependen de los estados de actualización. No se instalan automáticamente y deben ser aprobadas previamente por el administrador en la pestaña **Supervisión** en la Consola de administración (**Servidor de administración** `<nombre del servidor>` → **Supervisión**) o en la sección **Notificaciones** en Kaspersky Security Center Web Console (**Supervisión e informes** → **Notificaciones**). Después de eso, el administrador debe ejecutar explícitamente la instalación de las actualizaciones.

10. **Configurar la instalación automática de actualizaciones para las aplicaciones de seguridad**

    Cree tareas *Actualizar* para las aplicaciones administradas a fin de mantener al día las aplicaciones, los módulos de software y las bases de datos de Kaspersky (incluidas las bases de datos antivirus). Para evitar demoras en la instalación de actualizaciones, recomendamos que seleccione la opción **Al descargar nuevas actualizaciones al repositorio** al configurar la programación de la tarea.

    Si su red incluye dispositivos solo IPv6 y quiere actualizar regularmente las aplicaciones de seguridad instaladas en dichos dispositivos, asegúrese de que el Servidor de administración (versión 13.2 en adelante) y el Agente de red (versión 13.2 en adelante) estén instalados en los dispositivos administrados.

De forma predeterminada, las actualizaciones para Kaspersky Endpoint Security para Windows y Kaspersky Endpoint Security para Linux se instalan solo si su estado se cambia a *Aprobada*. Puede cambiar los ajustes de actualización en la tarea *Actualizar*.

Si una actualización exige revisar y aceptar los términos del Contrato de licencia de usuario final, es necesario aceptar esos términos para proceder con la instalación. Una vez que se aceptan los términos, la actualización se puede propagar a los dispositivos administrados.

Instrucciones:

- Consola de administración: Instalación automática de actualizaciones de Kaspersky Endpoint Security en los dispositivos
- Kaspersky Security Center Web Console: Instalación automática de actualizaciones de Kaspersky Endpoint Security en los dispositivos

### Resultados

Al culminar este escenario, Kaspersky Security Center estará configurado para actualizar las bases de datos de Kaspersky y las aplicaciones de Kaspersky instaladas una vez que las actualizaciones se descarguen en el repositorio del Servidor de administración o en los repositorios de los puntos de distribución. Su siguiente tarea consistirá, entonces, en supervisar el estado de la red.

## Acerca de la actualización de las bases de datos, los módulos de software y las aplicaciones de Kaspersky

Para asegurarse de que la protección de sus servidores de administración y sus dispositivos administrados siempre esté al día, debe proporcionar actualizaciones para los siguientes elementos oportunamente:

- Las bases de datos y los módulos de software de Kaspersky

  Antes de descargar las bases de datos y los módulos de software de Kaspersky, Kaspersky Security Center verifica que haya acceso a los servidores de Kaspersky. Si los servidores DNS configurados en el sistema no permiten acceder a los servidores de Kaspersky, la aplicación utiliza servidores DNS públicos. Esto se hace para garantizar que las bases de datos antivirus se mantengan actualizadas y para que los dispositivos administrados no vean afectado su nivel de seguridad.

- Las aplicaciones de Kaspersky que se encuentren instaladas, incluidas las aplicaciones de seguridad y los componentes de Kaspersky Security Center

  Kaspersky Security Center le permite actualizar el Agente de red y las aplicaciones de Kaspersky instaladas en dispositivos cliente basados en Windows y en Linux automáticamente. No se admite la actualización sin interrupciones del Servidor de administración, Kaspersky Security Center Web Console y los complementos web de administración. Para actualizar estos componentes, debe descargar las últimas versiones desde el sitio web de Kaspersky y realizar la instalación manualmente.

Existen distintos esquemas para descargar las actualizaciones necesarias y distribuirlas a los dispositivos administrados. La elección de una u otra opción depende de la configuración de la red. Estas son las posibilidades:

- Utilizar una sola tarea: *Descargar actualizaciones en el repositorio del Servidor de administración*
- Utilizar dos tareas:
  - la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*
  - La tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*
- Utilizar una carpeta local, una carpeta compartida o un servidor FTP (método manual)
- Realizar una descarga directa desde los servidores de actualizaciones de Kaspersky a Kaspersky Endpoint Security en los dispositivos administrados
- Utilizar una carpeta local o de red si el Servidor de administración no tiene conexión a Internet

## Utilizando la tarea Descargar actualizaciones en el repositorio del Servidor de administración

En este esquema, Kaspersky Security Center descarga las actualizaciones a través de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. En redes pequeñas que contienen menos de trescientos dispositivos administrados en un solo segmento de red o menos de diez dispositivos administrados en cada segmento de red, las actualizaciones se distribuyen a los dispositivos administrados directamente desde el repositorio del Servidor de administración (vea la siguiente imagen).

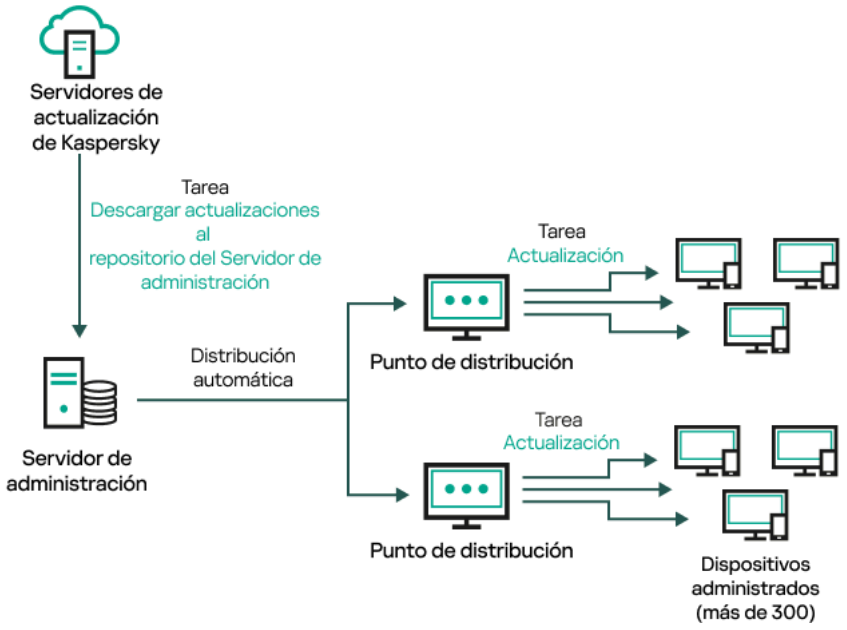



Actualización con la tarea Descargar actualizaciones en el repositorio del Servidor de administración sin utilizar puntos de distribución

De forma predeterminada, el Servidor de administración utiliza el protocolo HTTPS para comunicarse con los servidores de actualizaciones de Kaspersky y descargar las actualizaciones. Si lo desea, puede hacer que el Servidor de administración utilice el protocolo HTTP en lugar del protocolo HTTPS.

Si su red contiene más de trescientos dispositivos administrados en un solo segmento de red (o si su red consta de varios segmentos de red con más de nueve dispositivos administrados por segmento), le recomendamos que utilice puntos de distribución para propagar las actualizaciones a los dispositivos administrados (vea la siguiente imagen). Los puntos de distribución reducen la carga del Servidor de administración y optimizan el flujo de tráfico entre el Servidor de administración y los dispositivos administrados. Puede determinar cuántos puntos de distribución necesitará para su red y cuál deberá ser su configuración.

En este esquema, las actualizaciones se descargan automáticamente del repositorio del Servidor de administración a los repositorios de los puntos de distribución. Los dispositivos administrados incluidos en el alcance de un punto de distribución descargan las actualizaciones del repositorio de ese punto de distribución en lugar del repositorio del Servidor de administración.




Actualización con puntos de distribución y la tarea Descargar actualizaciones en el repositorio del Servidor de administración

Al completarse la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, se descargan las siguientes actualizaciones al repositorio del Servidor de administración:

- Bases de datos y módulos de software de Kaspersky para Kaspersky Security Center

  Estas actualizaciones se instalan automáticamente.

- Bases de datos y módulos de software de Kaspersky para las aplicaciones de seguridad instaladas en los dispositivos administrados

  Estas actualizaciones se instalan a través de la tarea "Actualizar" de Kaspersky Endpoint Security para Windows.

- Actualizaciones para el Servidor de administración

  Estas actualizaciones no se instalan automáticamente. El administrador debe aprobarlas e instalarlas manualmente.

  > Se requieren derechos de administrador local para instalar parches en el Servidor de administración.

- Actualizaciones para los componentes de Kaspersky Security Center

  Por defecto, estas actualizaciones se instalan automáticamente. Puede cambiar este comportamiento en la directiva del Agente de red.

- Actualizaciones para las aplicaciones de seguridad

  De forma predeterminada, Kaspersky Endpoint Security for Windows instala solo las actualizaciones que usted aprueba. Puede aprobar las actualizaciones mediante la Consola de administración o mediante Kaspersky Security Center Web Console. Las actualizaciones se instalan a través de la tarea *Actualizar* y se pueden configurar en las propiedades de dicha tarea.

> La tarea *Descargar actualizaciones en el repositorio del Servidor de administración* no está disponible en servidores de administración virtuales. El repositorio del Servidor de administración virtual muestra las actualizaciones descargadas al Servidor de administración principal.

Si lo desea, puede verificar el buen funcionamiento de las actualizaciones en un conjunto de dispositivos de prueba. De no encontrarse errores durante la verificación, las actualizaciones se distribuirán a otros dispositivos administrados.

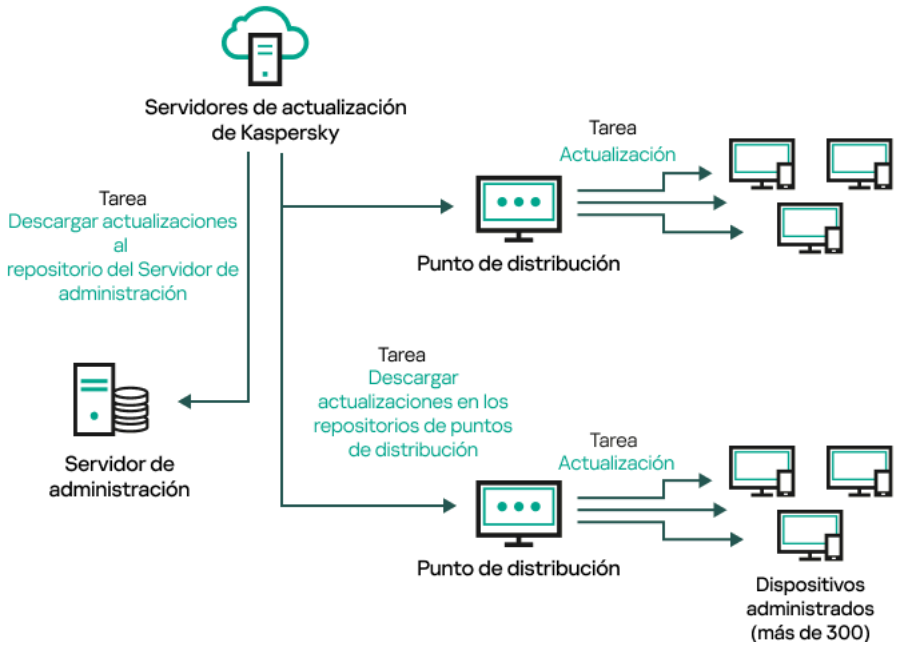
Cada aplicación de Kaspersky le solicita al Servidor de administración las actualizaciones que requiere. El Servidor de administración combina las solicitudes y descarga solo aquellas actualizaciones que han sido solicitadas por alguna aplicación. De este modo, se evita descargar la misma actualización más de una vez o descargar actualizaciones innecesarias. Para descargar las versiones correctas de las bases de datos y los módulos de software de Kaspersky, cuando se ejecuta la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, el Servidor de administración envía la siguiente información a los servidores de actualizaciones de Kaspersky automáticamente:

- Id. y versión de la aplicación
- Id. de instalación de la aplicación
- Id. de la clave activa
- Id. de ejecución de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*

La información transmitida no contiene datos personales ni confidenciales de ningún tipo. AO Kaspersky Lab protege la información conforme a las exigencias de la ley.

## Utilizar dos tareas: la tarea Descargar actualizaciones en el repositorio del Servidor de administración y la tarea Descargar actualizaciones en los repositorios de los puntos de distribución

Las actualizaciones pueden descargarse a los repositorios de los puntos de distribución directamente desde los servidores de actualizaciones de Kaspersky (y no desde el repositorio del Servidor de administración) y, una vez descargadas, pueden distribuirse a los dispositivos administrados (vea la siguiente imagen). Descargar las actualizaciones en los repositorios de los puntos de distribución es preferible cuando el Servidor de administración no tiene acceso a Internet o cuando transmitir datos entre el Servidor de administración y los puntos de distribución es más costoso que transmitir datos entre los puntos de distribución y los servidores de actualizaciones de Kaspersky.




Actualización con la tarea Descargar actualizaciones en el repositorio del Servidor de administración y la tarea Descargar actualizaciones en los repositorios de los puntos de distribución

De forma predeterminada, el Servidor de administración y los puntos de distribución se comunican con los servidores de actualizaciones de Kaspersky y descargan las actualizaciones utilizando el protocolo HTTPS. Puede hacer que el Servidor de administración y/o los puntos de distribución utilicen el protocolo HTTP en lugar del protocolo HTTPS.

Para implementar este esquema, cree la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución* además de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. Tras ello, los puntos de distribución descargarán las actualizaciones de los servidores de actualizaciones de Kaspersky y no del repositorio del Servidor de administración.

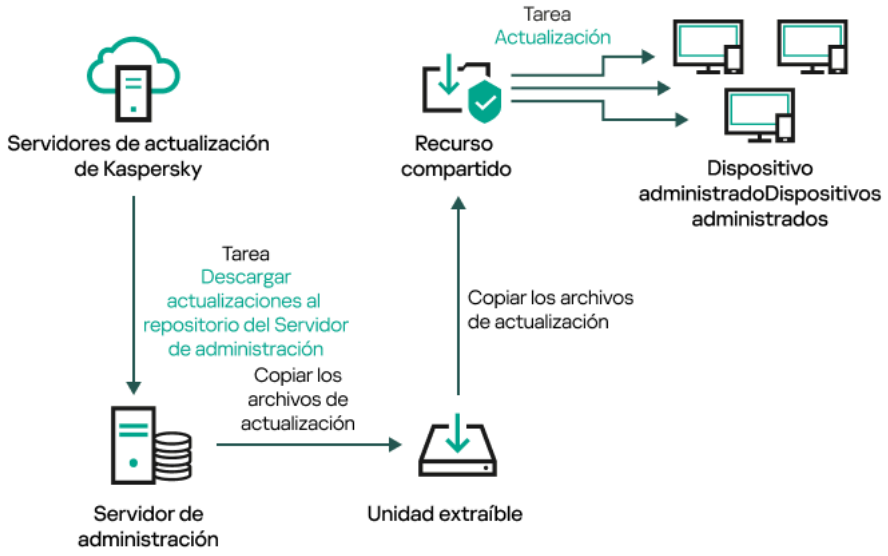
Los puntos de distribución con macOS no pueden descargar actualizaciones de los servidores de actualizaciones de Kaspersky.

Si hay uno o más dispositivos con macOS en el alcance de la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*, la tarea terminará con el estado *Error* aunque se complete sin errores en todos los dispositivos con Windows.

La tarea *Descargar actualizaciones en el repositorio del Servidor de administración* también es necesaria para este esquema, ya que se la utiliza para descargar las bases de datos y los módulos de software de Kaspersky para Kaspersky Security Center.

## Utilizar una carpeta local, una carpeta compartida o un servidor FTP (método manual)

Si sus dispositivos cliente no tienen conexión con el Servidor de administración, puede usar una carpeta local o un recurso compartido como origen de actualizaciones para actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky. De elegir esta alternativa, deberá copiar las actualizaciones requeridas del repositorio del Servidor de administración a una unidad extraíble y, luego, tendrá que copiar esas actualizaciones a la carpeta local o al recurso compartido que haya configurado como origen de actualizaciones en Kaspersky Endpoint Security (vea la siguiente imagen).



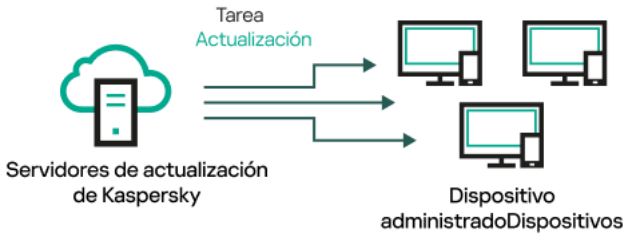

Actualización con una carpeta local, una carpeta compartida o un servidor FTP

Para obtener más información sobre los orígenes de actualizaciones en Kaspersky Endpoint Security, consulte los siguientes documentos de ayuda:

- Ayuda de Kaspersky Endpoint Security para Windows
- Ayuda de Kaspersky Endpoint Security for Linux

## Realizar una descarga directa desde los servidores de actualizaciones de Kaspersky a Kaspersky Endpoint Security en los dispositivos administrados

Puede configurar Kaspersky Endpoint Security en los dispositivos administrados para que la aplicación obtenga sus actualizaciones directamente de los servidores de actualizaciones de Kaspersky (vea la siguiente imagen).




Actualización directa de las aplicaciones de seguridad utilizando los servidores de actualizaciones de Kaspersky

En este esquema, la aplicación de seguridad no utiliza los repositorios que brinda Kaspersky Security Center. Para que las actualizaciones se descarguen directamente de los servidores de actualizaciones de Kaspersky, deberá definir esos servidores como origen de actualizaciones en la interfaz de la aplicación de seguridad. Para obtener más información acerca de estos ajustes, consulte los siguientes documentos de ayuda:

- Ayuda de Kaspersky Endpoint Security para Windows
- Ayuda de Kaspersky Endpoint Security for Linux

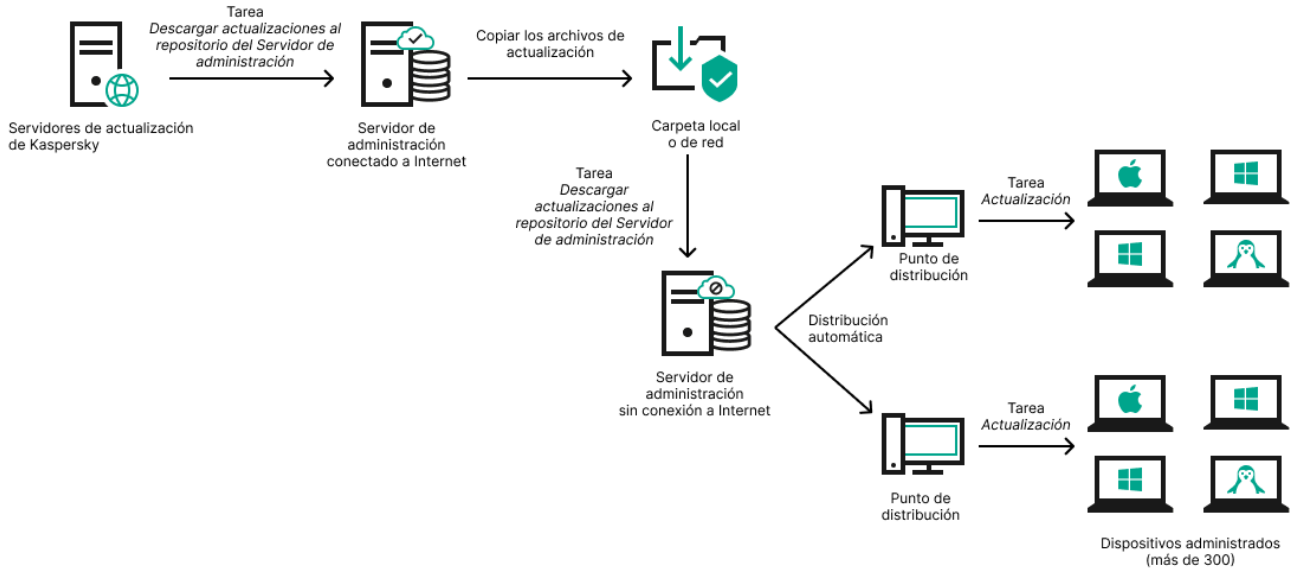
## Utilizar una carpeta local o de red si el Servidor de administración no tiene conexión a Internet

Si el Servidor de administración no tiene conexión a Internet, puede configurar la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* para descargar actualizaciones desde una carpeta local o de red. En este caso, de vez en cuando debe copiar los archivos de actualización necesarios en la carpeta especificada. Por ejemplo, puede copiar los archivos de actualización necesarios desde uno de los siguientes orígenes:

- Servidor de administración que cuente con una conexión a Internet (ver la figura a continuación)

  Dado que un Servidor de administración descarga solo las actualizaciones que solicitan las aplicaciones de seguridad, los conjuntos de aplicaciones de seguridad administrados por los Servidores de administración (el que tiene conexión a Internet y el que no) deben coincidir.

  Si el Servidor de administración que usa para descargar actualizaciones tiene la versión 13.2 o anterior, abra las propiedades de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* y, a continuación, habilite la opción **Descargar las actualizaciones usando el esquema antiguo**.




Utilizar una carpeta local o de red si el Servidor de administración no tiene conexión a Internet

- Kaspersky Update Utility

  Debido a que esta utilidad utiliza el antiguo esquema para descargar actualizaciones, abra las propiedades de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* y, a continuación, habilite la opción **Descargar las actualizaciones usando el esquema antiguo**.

# Crear la Descarga de actualizaciones para la tarea del repositorio del Servidor de administración

La tarea *Descargar actualizaciones en el repositorio del Servidor de administración* del Servidor de administración se crea automáticamente al utilizar el Asistente de inicio rápido de Kaspersky Security Center. Solo puede existir una copia de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. Por lo tanto, puede crear una tarea *Descargar actualizaciones en el repositorio del Servidor de administración* solo si esta tarea se eliminó de la lista de tareas del Servidor de administración.

Esta tarea es necesaria para descargar actualizaciones de los servidores de actualización de Kaspersky al repositorio del Servidor de administración. La lista de actualizaciones incluye lo siguiente:

- Actualizaciones de bases de datos y módulos de software para el Servidor de administración.
- actualizaciones para las bases de datos y los módulos de software de las aplicaciones de seguridad de Kaspersky.
- Actualizaciones a los componentes de Kaspersky Security Center.
- actualizaciones para las aplicaciones de seguridad de Kaspersky.

Una vez descargadas, las actualizaciones se pueden propagar a los dispositivos administrados.

Antes de que las actualizaciones se distribuyan a los dispositivos administrados, puede ejecutarse la tarea *Verificación de actualizaciones*. A través de esta tarea, puede asegurarse de que el Servidor de administración instalará las actualizaciones descargadas correctamente y de que el nivel de seguridad no disminuirá debido a las actualizaciones. Para que las actualizaciones se verifiquen antes de ser distribuidas, defina la opción **Ejecutar verificación de actualizaciones** en la configuración de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*.

*Para crear la tarea **Descargar actualizaciones en el repositorio del Servidor de administración**:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.
3. Para la aplicación Kaspersky Security Center, seleccione el tipo de tarea **Descargar actualizaciones en el repositorio del Servidor de administración**.
4. Escriba un nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).
5. Si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.
6. Haga clic en el botón **Crear**.

   Se crea la tarea y se la agrega a la lista de tareas.

7. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.

8. En la ventana de propiedades de la tarea, en la pestaña **Configuración de la aplicación**, especifique la siguiente configuración:

- Orígenes de actualizaciones

  Los siguientes recursos pueden utilizarse como orígenes de actualizaciones para el Servidor de administración:

  - Servidores de actualizaciones de Kaspersky

    Servidores HTTP(S) de Kaspersky desde los que las aplicaciones de Kaspersky descargan actualizaciones para sus bases de datos y módulos de software. De forma predeterminada, el Servidor de administración utiliza el protocolo HTTPS para comunicarse con los servidores de actualizaciones de Kaspersky y descargar las actualizaciones. Si lo desea, puede hacer que el Servidor de administración utilice el protocolo HTTP en lugar del protocolo HTTPS.

    Esta es la opción seleccionada por defecto.

  - Servidor de administración principal

    Este recurso se aplica a las tareas creadas para un Servidor de administración secundario o virtual.

  - Carpeta local o de red

    Una carpeta local o de red con las últimas actualizaciones. La carpeta de red puede ser un servidor FTP o HTTP, o un recurso compartido SMB. Si el acceso a la carpeta requiere autenticación, solo puede usarse el protocolo SMB. La carpeta local debe ser una carpeta del dispositivo en el que se encuentra instalado el Servidor de administración.

    > El servidor FTP/HTTP o la carpeta de red utilizada por un origen de actualizaciones debe contener una estructura de carpetas (con actualizaciones) que coincida con la estructura que se crea al usar los servidores de actualizaciones de Kaspersky.

  En caso de que una carpeta compartida que contenga actualizaciones esté protegida con contraseña, habilite la opción **Definir cuenta para acceder a la carpeta compartida del origen de actualizaciones (si corresponde)** e ingrese las credenciales de cuenta requeridas para el acceso.

- Carpeta para almacenar actualizaciones

  La ruta a la carpeta especificada para almacenar las actualizaciones guardadas. Puede copiar la ruta de la carpeta especificada en el portapapeles. No puede cambiar la ruta a una carpeta específica para una tarea de grupo.

- Otras opciones:

  - Forzar actualización de los Servidores de administración secundarios

    Si esta opción está habilitada, el Servidor de administración iniciará las tareas de actualización en los servidores de administración secundarios en cuanto se descarguen nuevas actualizaciones. Las tareas de actualización se inician utilizando el origen de actualización configurado en las propiedades de la tarea en los Servidores de administración secundarios.

    Si esta opción no está habilitada, las tareas de actualización se iniciarán en los Servidores de administración secundarios siguiendo lo que indiquen sus programaciones.

    Esta opción está deshabilitada de forma predeterminada.

- **Copiar actualizaciones descargadas a carpetas adicionales**

  Una vez que el Servidor de administración recibe actualizaciones, las copiará a las carpetas especificadas. Utilice esta opción si desea controlar manualmente la distribución de actualizaciones en la red.

  Podría utilizar esta opción en, por ejemplo, la siguiente situación: la red de su organización está formada por varias subredes independientes. Los dispositivos de cada subred no tienen acceso a las demás subredes. Sin embargo, los dispositivos de todas las subredes tienen acceso a una misma carpeta compartida. En un caso así, puede hacer que el Servidor de administración de una subred descargue las actualizaciones de los servidores de actualizaciones de Kaspersky, habilitar esta opción y definir esa carpeta compartida como destino. Luego, defina esa carpeta como origen de actualizaciones en las tareas "Descargar actualizaciones en el repositorio del Servidor de administración" de los demás servidores de administración.

  Si selecciona copiar las actualizaciones descargadas a una carpeta local, debe especificar una carpeta en el dispositivo que tiene el Servidor de administración instalado. La ruta a la carpeta depende del sistema operativo del dispositivo. Dado que la carpeta local se encuentra en el Servidor de administración basado en Linux, debe especificar la ruta POSIX, por ejemplo: /path/to/dir.

  Cuando selecciona una carpeta de red que se encuentra en el Servidor de administración basado en Linux, debe montar la carpeta para garantizar el acceso a la carpeta de red con anticipación desde el dispositivo que tiene el Servidor de administración. El acceso a la carpeta se realiza mediante el protocolo de SMB.

  Esta opción está deshabilitada de forma predeterminada.

- **No forzar la actualización de los dispositivos y los Servidores de administración secundarios si la copia no se ha completado**

  Las tareas para descargas actualizaciones en los dispositivos cliente y en los servidores de administración secundarios no se iniciarán hasta que las actualizaciones hayan terminado de copiarse de la carpeta de actualización principal a las carpetas de actualización adicionales.

  Debe habilitar esta opción si sus dispositivos cliente y sus servidores de administración secundarios obtienen sus actualizaciones de carpetas de red adicionales.

  Esta opción está deshabilitada de forma predeterminada.

- **Contenido de las actualizaciones**:

  - **Descargar archivos diff**

    Esta opción habilita la función de descarga de archivos diff.

    Esta opción está deshabilitada de forma predeterminada.

- **Descargar actualizaciones utilizando el esquema anterior**

A partir de la versión 14, Kaspersky Security Center utiliza el nuevo esquema al descargar actualizaciones para bases de datos y módulos de software. Para que la aplicación descargue las actualizaciones utilizando el nuevo esquema, el origen de actualizaciones debe contener archivos de actualización con metadatos que sean compatibles con el nuevo esquema. Si el origen de actualizaciones elegido contiene archivos de actualización con metadatos que solo son compatibles con el esquema anterior, habilite la opción **Descargar actualizaciones utilizando el esquema anterior**. De lo contrario, la tarea de descarga de actualizaciones no podrá completarse.

Habilite esta opción si, por ejemplo, seleccionó una carpeta local o de red como origen de actualizaciones y los archivos de actualización de dicha carpeta fueron descargados por alguna de las siguientes aplicaciones:

- Kaspersky Update Utility

  Esta utilidad descarga actualizaciones utilizando el esquema antiguo.

- Kaspersky Security Center 13.2 o una versión anterior

  Suponga, por ejemplo, que uno de sus servidores de administración no tiene conexión a Internet. En ese caso, podría utilizar un segundo Servidor de administración (que tenga conexión a Internet) para descargar las actualizaciones. Luego, podría colocar los archivos descargados en una carpeta local o de red que el primer servidor de administración pueda usar como origen de actualizaciones. Si el segundo Servidor de administración es de versión 13.2 o anterior, habilite la opción **Descargar actualizaciones utilizando el esquema anterior** en la tarea para el primer Servidor de administración.

Esta opción está deshabilitada de forma predeterminada.

- **Ejecutar verificación de actualizaciones**

El Servidor de administración descarga las actualizaciones del origen, las guarda en un repositorio temporal y ejecuta la tarea definida en el campo **Tarea de verificación de actualizaciones**. Si la tarea se completa con éxito, las actualizaciones se copian desde el repositorio temporal a una carpeta compartida en el Servidor de administración y luego se distribuyen a todos los dispositivos para los cuales el Servidor de administración actúa como fuente de actualizaciones (tareas con el tipo de programación **Al descargar nuevas actualizaciones al repositorio** empezada). La tarea para descargar las actualizaciones en el repositorio terminará solo luego de que se complete la tarea *Verificación de actualizaciones*.

Esta opción está deshabilitada de forma predeterminada.

9. En la ventana de propiedades de la tarea, en la pestaña **Programación**, cree una programación para el inicio de la tarea. De ser necesario, configure los siguientes ajustes:

- Iniciar tarea:

  Seleccione y configure la programación según la cual se ejecutará la tarea.

  - Manual

    La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

    Esta opción está seleccionada de forma predeterminada.

  - Cada N minutos

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

    De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

  - Cada N horas

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

    De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

  - Cada N días

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

    De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

  - Por días de la semana

    La tarea se ejecutará periódicamente en los días de la semana y a la hora que indique.

    De manera predeterminada, la tarea se ejecutará todos los viernes a las 18:00:00.

  - Mensual

    La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

    Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

    Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

- **Cada mes en los días especificados de semanas seleccionadas**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  Por defecto, la hora de inicio es a las 18:00 y no se selecciona ningún día del mes.

  > Tenga en cuenta que no selecciona una fecha específica en el mes, ni el número de la semana (primera, segunda semana del mes), sino el número de secuencia del día de la semana dentro de un mes. Por ejemplo, si coloca el cursor en la celda Tu de la Primera fila, significa que la tarea se ejecutará el primer martes de cada mes nuevo.**MaPrimero**

  Puede seleccionar varios días de la semana.

- **Ante brotes de virus**

  La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para defensa del perímetro
  - Antivirus para sistemas de correo

  Por defecto, están seleccionados todos los tipos de aplicaciones.

  En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- **Al completarse otra tarea**

  La tarea actual se iniciará después de que se complete otra tarea. Esta opción solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

- **Ejecutar tareas no realizadas**

Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

Esta opción está deshabilitada de forma predeterminada.

- Utilizar retardo aleatorio automático para el inicio de tareas

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

- Utilizar el retardo aleatorio automático para el inicio de la tarea dentro de un intervalo de

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

  Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

- Detener la tarea si tarda más de

  Una vez que transcurra el período especificado, la tarea se detendrá automáticamente, se haya completado o no.

  Habilite esta opción si desea que las tareas que tarden mucho en completarse se interrumpan o se detengan.

  Esta opción está deshabilitada de forma predeterminada. El tiempo de ejecución por defecto para las tareas es de 120 minutos.

10. Haga clic en el botón **Guardar**.

    La tarea queda creada y configurada.

Cuando el Servidor de administración realiza la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, las actualizaciones de las bases de datos y los módulos de software se descargan desde el origen de las actualizaciones y se almacenan en la carpeta compartida del Servidor de administración. Si crea esta tarea para un grupo de administración, la misma se aplicará solamente a los agentes de red incluidos en el grupo de administración especificado.

Las actualizaciones se distribuyen a los dispositivos cliente y a los servidores de administración secundarios desde la carpeta compartida del Servidor de administración.

# Comprobar actualizaciones descargadas

Antes de instalar actualizaciones en sus dispositivos administrados, puede comprobar que las mismas no tengan errores o problemas de funcionamiento. Dispone para ello de la tarea *Verificación de actualizaciones*. La tarea *Verificación de actualizaciones* se ejecuta automáticamente cuando se realiza la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. El Servidor de administración descarga las actualizaciones del origen, las guarda en el repositorio temporal y ejecuta la tarea *Verificación de actualizaciones*. Si esta tarea se completa sin errores, las actualizaciones se copian del repositorio temporal a la carpeta compartida del Servidor de administración. De allí, se distribuyen a los dispositivos cliente que tienen el Servidor de administración como origen de actualizaciones.

Si, como resultado de la tarea *Verificación de actualizaciones*, se determina que las actualizaciones del repositorio temporal son incorrectas, o si la tarea *Verificación de actualizaciones* se completa con errores, las actualizaciones problemáticas no se copian a la carpeta compartida. El Servidor de administración guarda el conjunto de actualizaciones anterior. Además, las tareas que tienen el tipo de programación **Al descargar nuevas actualizaciones al repositorio** no se inician en ese momento. Dichas operaciones se llevarán a cabo en el siguiente inicio de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* si el análisis de las nuevas actualizaciones finaliza correctamente.

El conjunto de actualizaciones se considera inválido si una de las condiciones siguiente se cumple al menos en un dispositivo de prueba:

- Ocurrió un error de la tarea de actualización.
- El estado de protección en tiempo real de la aplicación de seguridad cambió después de haber aplicado las actualizaciones.
- Se detectó un objeto infectado mientras se ejecutaba la tarea de análisis a pedido.
- Se produjo un error en el tiempo de ejecución de la aplicación de Kaspersky.

Si estas condiciones no se cumplen en ninguno de los dispositivos de prueba, el conjunto de actualizaciones se considera válido y la tarea *Verificación de actualizaciones* se da por correctamente completada.

Antes de comenzar a crear la tarea *Verificación de actualizaciones*, complete estos pasos:

1. Cree un grupo de administración que contenga algunos dispositivos de prueba. El grupo se usará para verificar las actualizaciones.

   Recomendamos que los dispositivos del grupo tengan la protección más fiable posible y que su configuración de aplicaciones sea la más usual en la red. Con ello mejorará la fiabilidad de los análisis antivirus, aumentará la probabilidad de que se detecten virus y se reducirá la incidencia de falsos positivos. De encontrarse virus en los dispositivos de prueba, se considerará que la tarea *Verificación de actualizaciones* no se completó correctamente.

2. Cree las tareas de actualización y análisis antimalware para una aplicación compatible con Kaspersky Security Center, como Kaspersky Endpoint Security para Windows o Kaspersky Security for Windows Server. Cuando cree las tareas de actualización y análisis antimalware, seleccione el grupo de administración que contenga los dispositivos de prueba.

   La tarea *Verificación de actualizaciones* ejecutará las tareas de actualización y análisis antimalware secuencialmente en los dispositivos de prueba para verificar que todas las actualizaciones sean válidas. Cuando cree la tarea *Verificación de actualizaciones*, deberá seleccionar las tareas de actualización y análisis antimalware que se ejecutarán.

3. Cree la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*.

*Para que Kaspersky Security Center verifique las actualizaciones descargadas antes de distribuirlas a los dispositivos cliente:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en la tarea **Descargar actualizaciones en el repositorio del Servidor de administración**.
3. En la ventana de propiedades de la tarea, vaya a la pestaña **Configuración de la aplicación** y habilite la opción **Ejecutar verificación de actualizaciones**.
4. Si la tarea *Verificación de actualizaciones* ya existe, haga clic en el botón **Elija una tarea**. En la ventana que se abre, seleccione la tarea *Verificación de actualizaciones* del grupo de administración con los dispositivos de prueba.

5. Si aún no creó la tarea *Verificación de actualizaciones*, haga lo siguiente:

   a. Haga clic en el botón **Nueva tarea**.

   b. Se abre el Asistente para crear nueva tarea. Escriba un nombre para la tarea (si desea cambiar el nombre predeterminado).

   c. Seleccione el grupo de administración con dispositivos de prueba que creó en un paso anterior.

   d. Primero, seleccione la tarea de actualización de una aplicación pertinente compatible con Kaspersky Security Center y luego seleccione la tarea de análisis antimalware.

   Hecho esto, aparecerán las siguientes opciones. Recomendamos que las deje habilitadas.

   - **Reiniciar el dispositivo después de la actualización de las bases de datos**

     Cuando se actualizan las bases de datos antivirus de un dispositivo, es recomendable reiniciarlo.

     La opción está habilitada de forma predeterminada.

   - **Comprobar el estado de la protección en tiempo real una vez que se actualice la base de datos y se reinicie el dispositivo**

     Si esta opción está habilitada, la tarea *Verificación de actualizaciones* comprobará si las actualizaciones descargadas en el repositorio del Servidor de administración son válidas y si el nivel de protección disminuyó tras actualizar las bases de datos antivirus y reiniciar el dispositivo.

     Esta opción está activada de forma predeterminada.

   e. Indique qué cuenta se usará para ejecutar la tarea *Verificación de actualizaciones*. Puede usar su propia cuenta y dejar la opción **Cuenta predeterminada** habilitada. Como alternativa, puede elegir otra cuenta que tenga los derechos de acceso necesarios para ejecutar la tarea. Para ello, haga clic en **Especificar cuenta** e ingrese las credenciales de la cuenta que desee usar.

6. Haga clic en **Guardar** para cerrar la ventana de propiedades de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*.

La verificación de actualización automática está habilitada. Ahora puede ejecutar la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* y comenzará desde la verificación de actualizaciones.

# Creación de la tarea Descargar actualizaciones en los repositorios de los puntos de distribución

Para que la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución* funcione en un dispositivo designado como punto de distribución, dicho dispositivo debe ejecutar Windows. Los puntos de distribución con Linux o macOS no pueden descargar actualizaciones de los servidores de actualizaciones de Kaspersky. Si al menos un dispositivo que ejecuta Linux o macOS está dentro del alcance de la tarea, la tarea tendrá el estado *Fallido*. Incluso si la tarea se completa correctamente en todos los dispositivos Windows, generará un error en los dispositivos restantes.

Puede crear la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución* para un grupo de administración. Cuando la tarea se ejecute, afectará a los puntos de distribución que formen parte del grupo de administración seleccionado.

Puede usar esta tarea, por ejemplo, si el tráfico entre el Servidor de administración y los puntos de distribución es más costoso que el tráfico entre los puntos de distribución y los servidores de actualización de Kaspersky, o si el Servidor de administración no tiene acceso a Internet.

Esta tarea se necesita para descargar actualizaciones de los servidores de actualizaciones de Kaspersky en los repositorios de los puntos de distribución. La lista de actualizaciones incluye lo siguiente:

- actualizaciones para las bases de datos y los módulos de software de las aplicaciones de seguridad de Kaspersky.
- Actualizaciones a los componentes de Kaspersky Security Center.
- actualizaciones para las aplicaciones de seguridad de Kaspersky.

Una vez descargadas, las actualizaciones se pueden propagar a los dispositivos administrados.

Si los puntos de distribución se conectan a Internet mediante un servidor proxy, debe especificar la configuración correspondiente en la directiva del Agente de red.

*Para crear la tarea **Descargar actualizaciones en los repositorios de los puntos de distribución** para un grupo de administración seleccionado:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en el botón **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.
3. Para la aplicación Kaspersky Security Center, en el campo **Tipo de tarea** seleccione **Descargar actualizaciones en los repositorios de los puntos de distribución**.
4. Escriba un nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).
5. Seleccione un botón de opción para elegir el grupo de administración, la selección de dispositivos o los dispositivos a los que se aplicará la tarea.
6. En el paso **Finalizar la creación de la tarea**, si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.
7. Haga clic en el botón **Crear**.

   Se crea la tarea y se la agrega a la lista de tareas.
8. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.

9. En la pestaña **Configuración de la aplicación** de la ventana de propiedades de la tarea, configure los siguientes ajustes:

- **Orígenes de actualizaciones**

  Los siguientes recursos se pueden utilizar como orígenes de actualizaciones para el punto de distribución:

  - Servidores de actualizaciones de Kaspersky

    Servidores HTTP(S) de Kaspersky desde los que las aplicaciones de Kaspersky descargan actualizaciones para sus bases de datos y módulos de software.

    Esta opción está seleccionada de forma predeterminada.

  - Carpeta local o de red

    Una carpeta local o de red con las últimas actualizaciones. La carpeta de red puede ser un servidor FTP o HTTP, o un recurso compartido SMB. Si el acceso a la carpeta requiere autenticación, solo puede usarse el protocolo SMB. La carpeta local debe ser una carpeta del dispositivo en el que se encuentra instalado el Servidor de administración.

    El servidor FTP/HTTP o la carpeta de red utilizada por un origen de actualizaciones debe contener una estructura de carpetas (con actualizaciones) que coincida con la estructura que se crea al usar los servidores de actualizaciones de Kaspersky.

- **Carpeta para almacenar actualizaciones**

  La ruta a la carpeta especificada para almacenar las actualizaciones guardadas. Puede copiar la ruta de la carpeta especificada en el portapapeles. No puede cambiar la ruta a una carpeta específica para una tarea de grupo.

- **Descargar archivos diff**

  Esta opción habilita la función de descarga de archivos diff.

  Esta opción está deshabilitada de forma predeterminada.

- **Descargar actualizaciones utilizando el esquema anterior**

A partir de la versión 14, Kaspersky Security Center utiliza el nuevo esquema al descargar actualizaciones para bases de datos y módulos de software. Para que la aplicación descargue las actualizaciones utilizando el nuevo esquema, el origen de actualizaciones debe contener archivos de actualización con metadatos que sean compatibles con el nuevo esquema. Si el origen de actualizaciones elegido contiene archivos de actualización con metadatos que solo son compatibles con el esquema anterior, habilite la opción **Descargar actualizaciones utilizando el esquema anterior**. De lo contrario, la tarea de descarga de actualizaciones no podrá completarse.

Habilite esta opción si, por ejemplo, seleccionó una carpeta local o de red como origen de actualizaciones y los archivos de actualización de dicha carpeta fueron descargados por alguna de las siguientes aplicaciones:

- Kaspersky Update Utility

  Esta utilidad descarga actualizaciones utilizando el esquema antiguo.

- Kaspersky Security Center 13.2 o una versión anterior

  Suponga, por ejemplo, que un punto de distribución está configurado para tomar las actualizaciones de una carpeta local o de red. En ese caso, puede utilizar un Servidor de administración que tenga conexión a Internet para descargar las actualizaciones y colocar los archivos descargados en la carpeta local del punto de distribución. Si el Servidor de administración es de versión 13.2 o anterior, habilite la opción **Descargar actualizaciones utilizando el esquema anterior** en la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*.

Esta opción está deshabilitada de forma predeterminada.

10. Programe la ejecución de la tarea. De ser necesario, configure los siguientes ajustes:

- **Iniciar tarea**

  Seleccione y configure la programación según la cual se ejecutará la tarea.

  - **Manual**

    La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

    Esta opción está seleccionada de forma predeterminada.

  - **Cada N minutos**

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

    De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

  - **Cada N horas**

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

    De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

  - **Cada N días**

    La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

    De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

  - **Por días de la semana**

    La tarea se ejecutará periódicamente en los días de la semana y a la hora que indique.

    De manera predeterminada, la tarea se ejecutará todos los viernes a las 18:00:00.

  - **Mensual**

    La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

    Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

    Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

  - **Cada mes en los días especificados de semanas seleccionadas**

La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

Por defecto, la hora de inicio es a las 18:00 y no se selecciona ningún día del mes.

Tenga en cuenta que no selecciona una fecha específica en el mes, ni el número de la semana (primera, segunda semana del mes), sino el número de secuencia del día de la semana dentro de un mes. Por ejemplo, si coloca el cursor en la celda **Ma** de la **Primero** fila, significa que la tarea se ejecutará el primer Martes de cada mes nuevo.

Puede seleccionar varios días de la semana.

- Ante brotes de virus

  La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para defensa del perímetro
  - Antivirus para sistemas de correo

  Por defecto, están seleccionados todos los tipos de aplicaciones.

  En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- Al completarse otra tarea

  La tarea actual se iniciará después de que se complete otra tarea. Esta opción solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

- Ejecutar tareas no realizadas

Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

Esta opción está deshabilitada de forma predeterminada.

- Utilizar retardo aleatorio automático para el inicio de la tarea

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

- Utilizar el retardo aleatorio automático para el inicio de la tarea dentro de un intervalo de

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

  Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

11. Haga clic en el botón **Guardar**.

    La tarea queda creada y configurada.

    Además de los ajustes configurados durante el proceso de creación, la tarea tiene otras propiedades que se pueden modificar.

Cuando se ejecuta la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*, las actualizaciones para las bases de datos y los módulos de software se descargan del origen de actualizaciones y se almacenan en la carpeta compartida. Las actualizaciones descargadas solo serán utilizadas por los puntos de distribución que formen parte del grupo de administración especificado y que no tengan una tarea de descarga de actualizaciones explícitamente definida para ellos.

# Habilitación y deshabilitación de actualizaciones automáticas y parches para componentes de Kaspersky Security Center

Las actualizaciones y las revisiones para el Servidor de administración solo se pueden instalar manualmente, después de obtener la aprobación explícita del administrador.

La instalación automática de actualizaciones y parches para componentes de Kaspersky Security Center está habilitada de forma predeterminada durante la instalación del Agente de red en el dispositivo. Puede deshabilitarla durante la instalación del Agente de red o más adelante usando una directiva.

*Para deshabilitar la actualización automática y los parches para componentes de Kaspersky Security Center durante instalación local del Agente de red en un dispositivo, realice lo siguiente:*

1. Inicie la instalación local del Agente de red en el dispositivo.
2. En el paso **Configuración avanzada**, desactive la casilla **Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes**.
3. Siga las instrucciones del asistente.

   Se instalará el Agente de red con la actualización automática y los parches para componentes de Kaspersky Security Center deshabilitados en el dispositivo. Si desea habilitar la autoinstalación de actualizaciones y parches más adelante, podrá hacerlo a través de una directiva.

*Para deshabilitar la actualización automática y los parches para componentes de Kaspersky Security Center durante la instalación del Agente de red en el dispositivo mediante un paquete de instalación, realice lo siguiente:*

1. En el menú principal, vaya a **Operaciones → Repositorios → Paquetes de instalación**.
2. Haga clic en el paquete **Agente de red de Kaspersky Security Center <número de versión>**.
3. En la ventana de propiedades, abra la pestaña **Configuración**.
4. Desactive el interruptor **Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes**.

   Se instalará el Agente de red con la actualización automática y los parches para componentes de Kaspersky Security Center deshabilitados de este paquete. Si desea habilitar la autoinstalación de actualizaciones y parches más adelante, podrá hacerlo a través de una directiva.

Si esta casilla se seleccionó (o se desactivó) durante la instalación del Agente de red en el dispositivo, puede habilitar posteriormente (o deshabilitar) la actualización automática usando la directiva del Agente de red.

*Para habilitar o deshabilitar la actualización automática y los parches para componentes de Kaspersky Security Center usando la directiva del Agente de red, realice lo siguiente:*

1. En el menú principal, vaya a **Activos (dispositivos) → Directivas y perfiles**.
2. Haga clic en la directiva del Agente de red.

3. En la ventana de propiedades de la directiva, vaya a la pestaña **Configuración de la aplicación**.

4. En la sección **Administrar parches y actualizaciones**, active o desactive el interruptor **Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes** para habilitar o deshabilitar, respectivamente, la instalación automática de actualizaciones y parches.

5. Bloquee (🔒) el interruptor.

La directiva se aplicará a los dispositivos seleccionados y la actualización automática y los parches para los componentes de Kaspersky Security Center se habilitarán (o se deshabilitarán) en estos dispositivos.

# Instalación automática de actualizaciones para Kaspersky Endpoint Security para Windows

Puede hacer que las bases de datos y los módulos de software de Kaspersky Endpoint Security para Windows se actualicen automáticamente en los dispositivos cliente.

*Para que las actualizaciones de Kaspersky Endpoint Security para Windows se descarguen y se instalen automáticamente en los dispositivos cliente, haga lo siguiente:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.

2. Haga clic en el botón **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.

3. Busque la aplicación Kaspersky Endpoint Security para Windows y seleccione **Actualizar** como subtipo de tarea.

4. Escriba un nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).

5. Elija el alcance de la tarea.

6. Elija el grupo de administración, la selección de dispositivos o los dispositivos a los que se aplicará la tarea.

7. En el paso **Finalizar la creación de la tarea**, si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.

8. Haga clic en el botón **Crear**.

   Se crea la tarea y se la agrega a la lista de tareas.

9. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.

10. En la pestaña **Configuración de la aplicación** de la ventana de propiedades de la tarea, defina la configuración de la tarea de actualización en modo local o modo móvil:

    - **Modo local**: existe una conexión entre el dispositivo y el Servidor de administración.

    - **Modo móvil**: No se establece conexión entre Kaspersky Security Center y el dispositivo (por ejemplo, cuando el dispositivo no está conectado a Internet).

11. Habilite los orígenes de actualizaciones que desee usar para actualizar las bases de datos y los módulos de Kaspersky Endpoint Security para Windows. Si es necesario, cambie las posiciones de las fuentes en la lista usando con los botones **Subir** y **Bajar**. Si habilita más de un origen de actualizaciones, Kaspersky Endpoint Security para Windows intentará conectarse a ellos en orden, uno tras otro, comenzando por el primero de la lista. La tarea de actualización descargará el paquete de actualización del primer origen disponible.

12. Habilite la opción **Instalar actualizaciones aprobadas para los módulos de la aplicación** para que, junto con las bases de datos de la aplicación, se descarguen también las actualizaciones para los módulos de software.

    Si habilita esta opción, Kaspersky Endpoint Security para Windows le informará al usuario sobre la disponibilidad de actualizaciones para los módulos de software. Cuando se ejecute la tarea de actualización, estas actualizaciones se incluirán en el paquete de actualización. Kaspersky Endpoint Security para Windows instala solo aquellas actualizaciones para las cuales ha establecido el estado *Aprobado*; se instalarán localmente a través de la interfaz de la aplicación o de Kaspersky Security Center.

    También puede habilitar la opción **Instalar automáticamente actualizaciones de módulos críticas**. Cuando haya actualizaciones disponibles para los módulos de software, Kaspersky Endpoint Security para Windows instalará automáticamente las que tengan estado *Crítico*; las demás actualizaciones se instalarán cuando usted las apruebe.

    Para actualizar los módulos de software, podría resultar necesario leer y aceptar los términos del contrato de licencia y la política de privacidad. Cuando este sea el caso, la aplicación esperará a que el usuario acepte los términos de estos documentos y luego instalará las actualizaciones.

13. Marque la casilla **Copiar actualizaciones a la siguiente carpeta** para que la aplicación guarde las actualizaciones descargadas en una carpeta. A continuación, elija la carpeta de destino.

14. Defina una programación para la tarea. Recomendamos seleccionar la opción **Al descargar nuevas actualizaciones al repositorio** de manera que las actualizaciones se instalen sin demora.

15. Haga clic en **Guardar**.

Cuando la tarea **Actualizar** está en ejecución, la aplicación envía solicitudes a los servidores de actualizaciones de Kaspersky.

Algunas actualizaciones requieren que estén instaladas las últimas versiones de los complementos de administración.

# Aprobar y rechazar actualizaciones de software

Una tarea de instalación de actualizaciones puede estar configurada para requerir la aprobación de las actualizaciones que se deban instalar. Puede aprobar las actualizaciones que deban instalarse y rechazar las que no deban instalarse.

Podría suceder, por ejemplo, que quiera instalar las actualizaciones en un entorno de prueba para verificar primero que no interfieran con el funcionamiento de los dispositivos, y solo entonces, en caso de no haber problemas, permitir que se instalen en los dispositivos cliente.

La posibilidad de aprobar y rechazar actualizaciones solo está disponible para el Agente de red y las aplicaciones administradas instaladas en los dispositivos cliente basados en Windows. No se admite la actualización sin interrupciones del Servidor de administración, Kaspersky Security Center Web Console y los complementos web de administración. Para actualizar estos componentes, debe descargar las últimas versiones desde el sitio web de Kaspersky y realizar la instalación manualmente.

*Para aprobar o rechazar una o más actualizaciones:*

1. En el menú principal, vaya a **Operaciones → Aplicaciones de Kaspersky → Actualizaciones sin interrupciones**.

   Se mostrará una lista con las actualizaciones disponibles.

   Las actualizaciones para las aplicaciones administradas pueden requerir que la versión de Kaspersky Security Center instalada sea posterior a una versión en particular. Si está utilizando una versión anterior a la necesaria, podrá ver estas actualizaciones, pero no las podrá aprobar. Tampoco podrá crear paquetes de instalación a partir de esas actualizaciones hasta que actualice Kaspersky Security Center. Si intenta hacerlo, se le pedirá que actualice su copia de Kaspersky Security Center a la versión mínima requerida.

2. Seleccione las actualizaciones que desee aprobar o rechazar.

3. Haga clic en **Aprobar** para aprobar las actualizaciones seleccionadas o en **Rechazar** para rechazarlas.

   El valor predeterminado es *Sin definir*.

Las actualizaciones a las que les asigne el estado *Aprobada* se pondrán en una cola para ser instaladas.

Las actualizaciones a las que les asigne el estado *Rechazada* se desinstalarán (si tal acción es posible) de todos los dispositivos en los que estén instaladas. Estas actualizaciones no se instalarán en otros dispositivos en el futuro.

Existen actualizaciones para las aplicaciones de Kaspersky que no se pueden desinstalar. Si configura el estado *Rechazada* para ellas, Kaspersky Security Center no desinstalará estas actualizaciones de los dispositivos en los cuales se hayan instalado anteriormente. Sin embargo, se abstendrá de instalarlas en otros dispositivos en el futuro.

Si asigna el estado *Rechazada* a las actualizaciones de software de un tercero, estas no se instalarán en los dispositivos a los que estén asignadas, pero que aún no las hayan recibido. Las actualizaciones no se eliminarán de los dispositivos en los que ya se encuentren instaladas. Si necesita eliminarlas, deberá hacerlo manualmente, en forma local.

# Actualización del Servidor de administración

Puede instalar las actualizaciones del Servidor de administración mediante el uso de Asistente de actualización del Servidor de administración.

*Para instalar una actualización del Servidor de administración:*

1. En el menú principal, vaya a **Operaciones→ Aplicaciones de Kaspersky → Actualizaciones sin interrupciones**.
2. Ejecute Asistente de actualización del Servidor de administración de una de las siguientes formas:
   - Haga clic en el nombre de una actualización del Servidor de administración en la lista de actualizaciones, y en la ventana que se abre, haga clic en el vínculo **Ejecutar el Asistente de actualización del Servidor de administración**.
   - Haga clic en el vínculo **Ejecutar el Asistente de actualización del Servidor de administración** en el campo de notificaciones en la parte superior de la ventana.
3. En la ventana Asistente de actualización del Servidor de administración, seleccione una de las siguientes opciones para especificar cuando desea instalar una actualización:
   - **Instalar ahora**. Seleccione esta opción si desea instalar la actualización ahora.
   - **Posponer la instalación**. Seleccione esta opción si desea instalar la actualización más adelante. En esta caso, aparecerá una notificación sobre esta actualización.
   - **Ignorar actualización**. Seleccione esta opción si no desea instalar una actualización y no desea recibir notificaciones sobre esta actualización.
4. Seleccione la opción **Crear una copia de seguridad del Servidor de administración antes de instalar actualizaciones** si desea crear una copia de seguridad del Servidor de administración antes de instalar la actualización.
5. Haga clic en el botón **Aceptar** para finalizar el asistente.

Si se interrumpe el proceso de creación de copia de seguridad, también se interrumpe el proceso de instalación de la actualización.

# Habilitación y deshabilitación del modelo de descarga de actualizaciones sin conexión

Recomendamos que evite deshabilitar el modelo de descarga de actualizaciones sin conexión. Deshabilitarlo puede causar fallos en la entrega de actualización a dispositivos. En ciertos casos, un especialista del Servicio de soporte técnico de Kaspersky puede recomendar que desactive la opción **Descargar actualizaciones y bases de datos antivirus del Servidor de administración con anticipación**. En este caso, tendrá que asegurarse de que la tarea para recibir actualizaciones para aplicaciones de Kaspersky esté configurada.

*Para habilitar o deshabilitar el modelo de descarga de actualizaciones sin conexión para un grupo de administración:*

1. En el menú principal, vaya a **Activos (dispositivos) → Directivas y perfiles**.
2. Haga clic en **Grupos**.

3. En la estructura del grupo de administración, seleccione el grupo de administración para el que desea configurar el modelo de descarga de actualizaciones sin conexión.

4. Haga clic en la directiva del Agente de red.

   Se abre la ventana de propiedades de la directiva del Agente de red.

   > De forma predeterminada, la configuración de las directivas secundarias se hereda de las directivas principales y no se puede modificar. Si la directiva que desea modificar se hereda, primero debe crear una nueva directiva para el Agente de red en el grupo de administración correspondiente. En la directiva recién creada, podrá modificar las opciones de configuración que no estén bloqueadas en la directiva principal.

5. En la pestaña **Configuración de la aplicación**, seleccione la sección **Administrar parches y actualizaciones**.

6. Habilite o deshabilite la opción **Descargar actualizaciones y bases de datos antivirus del Servidor de administración con anticipación (recomendado)** para habilitar o deshabilitar, respectivamente, el modelo de descarga de actualizaciones sin conexión.

   De manera predeterminada, el modelo de descarga sin conexión está habilitado.

El modelo de descarga de actualizaciones sin conexión se habilitará o se deshabilitará.

# Actualizar las bases de datos y los módulos de software de Kaspersky en dispositivos sin conexión

Para que los dispositivos administrados siempre estén protegidos contra virus y otras amenazas, es muy importante mantener al día las bases de datos y los módulos de software de las aplicaciones de Kaspersky instaladas. Los administradores generalmente configuran actualizaciones regulares mediante el uso del repositorio del Servidor de administración o repositorios de puntos de distribución.

Cuando necesite una actualización de las bases de datos y los módulos de software en un dispositivo (o un grupo de dispositivos) que no esté conectado al Servidor de administración (principal o secundario), a un punto de distribución o a Internet, tiene que usar fuentes alternativas de actualizaciones, como un servidor FTP o una carpeta local. En ese caso, tendrá que transferir los archivos de las actualizaciones utilizando una unidad de memoria, un disco duro externo u otro dispositivo de almacenamiento masivo.

Puede copiar las actualizaciones requeridas desde:

- Servidor de administración.

  Para asegurarse de que el repositorio del Servidor de administración contenga las actualizaciones necesarias para la aplicación de seguridad instalada en un dispositivo sin conexión, al menos uno de los dispositivos en línea administrados debe tener la misma aplicación de seguridad instalada. Esta aplicación debe estar configurada para recibir las actualizaciones desde el repositorio del Servidor de administración a través de la tarea Descargar actualizaciones en el repositorio del Servidor de administración.

- Cualquier dispositivo que tenga la misma aplicación de seguridad instalada y configurada para recibir las actualizaciones desde el repositorio del Servidor de administración, un repositorio de puntos de distribución o directamente desde los servidores de actualización de Kaspersky.

A continuación se muestra un ejemplo de configuración de actualizaciones de bases de datos y módulos de software al copiarlos desde el repositorio del Servidor de administración.

*Para actualizar las bases de datos y los módulos de software de Kaspersky en dispositivos sin conexión:*

1. Conecte la unidad extraíble al dispositivo donde está instalado el Servidor de administración.
2. Copie los archivos de las actualizaciones a la unidad extraíble.

   De forma predeterminada, las actualizaciones se localizan en: \\<nombre del servidor>\KLSHARE\Updates.

   O bien, puede configurar Kaspersky Security Center para copiar regularmente las actualizaciones a la carpeta que seleccione. La tarea Descargar actualizaciones en el repositorio del Servidor de administración ofrece para ello la opción **Copiar actualizaciones descargadas a carpetas adicionales**. Si elige, como carpeta de destino para esta opción, una carpeta ubicada en una unidad de memoria USB o en un disco duro externo, el dispositivo de almacenamiento masivo siempre contendrá la última versión de las actualizaciones.
3. En los dispositivos sin conexión, configure la aplicación de seguridad (por ejemplo, Kaspersky Endpoint Security para Windows) para que obtenga sus actualizaciones de una carpeta local o de un recurso compartido (por ejemplo, una carpeta compartida o un servidor FTP).
4. Copie los archivos de las actualizaciones de la unidad extraíble a la carpeta local o al recurso compartido que quiera usar como origen de actualizaciones.
5. En el dispositivo sin conexión en el que se deban instalar las actualizaciones, inicie la tarea de actualización de Kaspersky Endpoint Security para Windows.

Cuando se complete la tarea de actualización, el dispositivo tendrá las bases de datos y los módulos de software de Kaspersky más recientes.

# Copia de seguridad y restauración de complementos web

Kaspersky Security Center Web Console le permite hacer una copia de seguridad del estado actual de un complemento web para poder restaurar el estado guardado más tarde. Por ejemplo, puede hacer una copia de seguridad de un complemento web antes de actualizarlo a una versión más nueva. Después de la actualización, si la versión más reciente no cumple con sus requisitos o expectativas, puede restaurar la versión anterior del complemento web desde la copia de seguridad.

*Para hacer copias de seguridad de los complementos web:*

1. En el menú principal, vaya a **Configuración → Complementos web**.
2. En la sección **Complementos web**, seleccione los complementos web de los que desea realizar una copia de seguridad y, a continuación, haga clic en el botón **Crear una copia de seguridad**.

Se realiza una copia de seguridad de los complementos web seleccionados. Puede ver las copias de seguridad creadas en la sección **Copias de seguridad**.

*Para restaurar un complemento web desde una copia de seguridad:*

1. En el menú principal, vaya a **Configuración → Copias de seguridad**.
2. En la sección **Copias de seguridad**, seleccione la copia de seguridad del complemento web que desea restaurar y, a continuación, haga clic en el botón **Reinstalar desde la copia de seguridad**.

El complemento web se restaura a partir de la copia de seguridad seleccionada.

# Ajuste de puntos de distribución y puertas de enlace de conexión

Una estructura de grupos de administración en Kaspersky Security Center realiza las funciones siguientes:

- Define el alcance de las directivas

  Existe otra forma de aplicar ajustes pertinentes en dispositivos: mediante el uso de *perfiles de directiva*. En este caso, el alcance de las directivas se establece a través de etiquetas, ubicaciones de dispositivos en unidades organizativas de Active Directory o membresías en grupos de seguridad de Active Directory.

- Define el alcance de las tareas de grupo

  Existe un modo de definir el alcance de las tareas de grupo que no depende de una jerarquía de grupos de administración: el uso de tareas para selecciones de dispositivos y de tareas para dispositivos específicos.

- Regula la capacidad de acceder a los distintos dispositivos, Servidores de administración secundarios y Servidores de administración virtuales

- Asigna puntos de distribución

Al momento de crear la estructura de grupos de administración, para que la asignación de puntos de distribución sea óptima, es necesario tener en cuenta la topología de la red de la organización. La distribución óptima de puntos de distribución le permite ahorrar tráfico en la red de la organización.

Dependiendo del organigrama de la organización y de la topología de la red, pueden aplicarse las siguientes configuraciones estándares a la estructura de grupos de administración:

- Oficina única

- Varias oficinas remotas pequeñas

Los dispositivos designados como puntos de distribución deben protegerse contra el acceso no autorizado por medios virtuales y físicos.

## Configuración estándar de puntos de distribución: oficina única

En una configuración estándar de "oficina única", todos los dispositivos se encuentran en la red de la organización y tienen la capacidad de "verse" los unos a los otros. La red de la organización puede constar de varias partes independientes (redes o segmentos de red) vinculadas por canales estrechos.

Los siguientes métodos pueden emplearse para armar la estructura de grupos de administración:

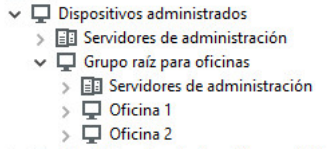
- Armar la estructura de grupos de administración tomando en cuenta la topología de la red. No es necesario que la estructura de grupos de administración refleje con absoluta precisión la topología de la red. Es suficiente con que haya coincidencia entre las partes independientes de la red y ciertos grupos de administración. Puede usar la asignación automática de puntos de distribución o asignarlos manualmente.

- Armar la estructura de grupos de administración sin tener en cuenta la topología de la red. En este caso, debe deshabilitar la asignación automática de puntos de distribución y luego asignar uno o varios dispositivos para que actúen como puntos de distribución para un grupo de administración original en cada una de las partes independientes de la red; por ejemplo, para el grupo **Dispositivos administrados**. Todos los puntos de distribución estarán al mismo nivel y presentarán el mismo alcance en todos los dispositivos en la red de la organización. En este caso, cada Agente de red se conectará al punto de distribución que tenga la ruta más corta. La ruta a un punto de distribución se puede determinar con la utilidad tracert.

## Configuración estándar de puntos de distribución: varias oficinas remotas pequeñas

Esta configuración estándar contempla la existencia de varias pequeñas oficinas remotas, que pueden comunicarse con una oficina central a través de Internet. Cada oficina remota está ubicada detrás de una pasarela NAT; debido a ello, las oficinas remotas están aisladas las unas de las otras y no se pueden conectar entre sí.

La configuración se debe ver reflejada en la estructura de grupos de administración: debe crearse un grupo de administración independiente para cada oficina remota (los grupos **Oficina 1** y **Oficina 2** en la siguiente imagen).




Oficinas remotas incluidas en la estructura de grupos de administración

Cada grupo de administración correspondiente a una oficina debe tener asignados uno o más puntos de distribución. Los puntos de distribución deben ser dispositivos que se encuentren en la oficina remota y deben tener una cantidad suficiente de espacio libre en disco. Los dispositivos incluidos en el grupo **Oficina 1** accederán a los puntos de distribución asignados al grupo de administración **Oficina 1**, por ejemplo.

Cuando hay usuarios que utilizan una computadora portátil para trabajar físicamente en más de una oficina, resulta necesario designar, junto con los puntos de distribución existentes, dos o más dispositivos en cada oficina remota para que actúen como puntos de distribución de un grupo de administración ubicado en un nivel superior (el grupo llamado **Grupo para oficinas** en la imagen anterior).

Ejemplo: Una computadora portátil incluida en el grupo de administración **Oficina 1** se traslada físicamente a la oficina que corresponde al grupo de administración **Oficina 2**. Luego del traslado, el Agente de red de la computadora portátil intenta acceder a los puntos de distribución asignados al grupo **Oficina 1**, pero esos puntos de distribución no están disponibles. Tras ello, el Agente de red intenta acceder a los puntos de distribución asignados al **Grupo para oficinas**. Como las oficinas remotas están aisladas entre sí, los intentos de acceder a los puntos de distribución asignados al grupo de administración **Grupo para oficinas** solo tendrán éxito cuando el Agente de red intente acceder a los puntos de distribución del grupo **Oficina 2**. Así, la computadora portátil permanecerá en el grupo de administración correspondiente a su oficina inicial, pero usará el punto de distribución de la oficina en la que se encuentre físicamente.

# Acerca de la asignación de puntos de distribución

Puede asignar un dispositivo administrado como punto de distribución de forma manual o automática.

Si asigna un dispositivo administrado como punto de distribución de forma manual, puede seleccionar cualquier dispositivo en su red.

Si asigna puntos de distribución de forma automática, Kaspersky Security Center puede seleccionar solo el dispositivo administrado que cumpla con las siguientes condiciones:

- El dispositivo tiene un mínimo de 50 GB de espacio de disco libre.
- El dispositivo administrado está conectado con Kaspersky Security Center directamente (no a través de la puerta de enlace).
- El dispositivo administrado no es una computadora portátil.

> Si su red no tiene dispositivos que cumplan con las condiciones especificadas, Kaspersky Security Center no asignará ningún dispositivo como punto de distribución de forma automática.

# Asignar puntos de distribución automáticamente

Recomendamos que asigne puntos de distribución automáticamente. En este caso, Kaspersky Security Center seleccionará por sí mismo qué dispositivos deben tener asignados puntos de distribución.

*Para asignar puntos de distribución automáticamente:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Puntos de distribución**.
3. Seleccione la opción **Asignar automáticamente puntos de distribución**.

   > Si la asignación automática de dispositivos como puntos de distribución está habilitada, no puede configurar los puntos de distribución manualmente ni editar la lista de puntos de distribución.

4. Haga clic en el botón **Guardar**.

El Servidor de administración asigna y configura los puntos de distribución automáticamente.

# Designación manual de puntos de distribución

Kaspersky Security Center le permite asignar manualmente dispositivos para actuar como puntos de distribución.

Recomendamos que asigne puntos de distribución automáticamente. En este caso, Kaspersky Security Center seleccionará por sí mismo qué dispositivos deben tener asignados puntos de distribución. Sin embargo, si tiene que optar por no asignar puntos de distribución automáticamente por cualquier motivo (por ejemplo, si desea utilizar servidores asignados exclusivamente), puede asignar puntos de distribución manualmente después de calcular su número y configuración.

Los dispositivos designados como puntos de distribución deben protegerse contra el acceso no autorizado por medios virtuales y físicos.

*Para designar manualmente un dispositivo como punto de distribución:*

1. En el menú principal, haga clic en el ícono de configuración (  ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Puntos de distribución**.

3. Seleccione la opción **Asignar manualmente puntos de distribución**.

4. Haga clic en el botón **Asignar**.

5. Seleccione el dispositivo que quiera designar como punto de distribución.

   A la hora de seleccionar un dispositivo, tenga presentes las características de funcionamiento de los puntos de distribución y los requisitos con los que debe cumplir un dispositivo para actuar como punto de distribución.

6. Seleccione el grupo de administración que desee incluir en el alcance del punto de distribución seleccionado.

7. Haga clic en el botón **Aceptar**.

   El punto de distribución agregado aparecerá en la lista de puntos de distribución, en la sección **Puntos de distribución**.

8. Haga clic en el punto de distribución recién agregado en la lista para abrir su ventana de propiedades.

9. En la ventana de propiedades, configure los ajustes del punto de distribución:

- La sección **General** contiene la configuración de interacción entre el punto de distribución y los dispositivos cliente:

  - **Puerto SSL**

    El número del puerto SSL que se usará para establecer una conexión cifrada con SSL entre el punto de distribución y los dispositivos cliente.

    De manera predeterminada, se utiliza el puerto 13000.

  - **Utilizar multidifusión**

    Si habilita esta opción, se utilizará la multidifusión IP para distribuir automáticamente los paquetes de instalación a los dispositivos cliente del grupo.

    Cuando necesite instalar una aplicación en un grupo de dispositivos cliente utilizando un paquete de instalación, la multidifusión IP ayudará a que el proceso se complete más rápidamente. Sin embargo, cuando se necesita instalar una aplicación en un único dispositivo cliente, la multidifusión hace que el tiempo de instalación aumente.

  - **Dirección de multidifusión IP**

    La dirección IP que se utilizará para la multidifusión. Puede usar cualquier dirección IP del intervalo 224.0.0.0-239.255.255.255

    De manera predeterminada, Kaspersky Security Center asignará automáticamente una dirección de multidifusión IP única tomada de este intervalo.

  - **Puerto para la multidifusión IP**

    Número del puerto que se usará para la multidifusión IP.

    El puerto por defecto es el 15001. De forma predeterminada, si el dispositivo que tiene instalado el Servidor de administración es, además, el punto de distribución designado, se usará el puerto 13001 para las conexiones SSL.

  - **Dirección del punto de distribución para dispositivos remotos**

    La dirección IPv4 a través de la cual los dispositivos remotos se conectan al punto de distribución.

  - **Desplegar actualizaciones**

Las actualizaciones se distribuirán a los dispositivos administrados desde las siguientes fuentes:

- si deja esta opción habilitada: el presente punto de distribución;
- si deshabilita esta opción: otros puntos de distribución, el Servidor de administración o los servidores de actualizaciones de Kaspersky.

Si utiliza puntos de distribución para distribuir las actualizaciones, reducirá el número de descargas y verá una merma en el volumen de tráfico. Además, al distribuir la carga entre los puntos de distribución, también logrará aminorar la carga del Servidor de administración. Puede calcular cuántos puntos de distribución necesitará en su red para reducir los volúmenes de tráfico y de carga.

Si deshabilita esta opción, el número de descargas de actualizaciones y la carga del Servidor de administración podrían aumentar. Esta opción está activada de forma predeterminada.

- **Desplegar paquetes de instalación**

  Los paquetes de instalación se distribuirán a los dispositivos administrados desde las siguientes fuentes:

  - si deja esta opción habilitada: el presente punto de distribución;
  - si deshabilita esta opción: otros puntos de distribución, el Servidor de administración o los servidores de actualizaciones de Kaspersky.

  Si utiliza puntos de distribución para desplegar los paquetes de instalación, reducirá el número de descargas y verá una merma en el volumen de tráfico. Además, al distribuir la carga entre los puntos de distribución, también logrará aminorar la carga del Servidor de administración. Puede calcular cuántos puntos de distribución necesitará en su red para reducir los volúmenes de tráfico y de carga.

  Si deshabilita esta opción, el número de descargas de paquetes de instalación y la carga del Servidor de administración podrían aumentar. Esta opción está activada de forma predeterminada.

- **Ejecutar servidor push**

  En Kaspersky Security Center, un punto de distribución puede funcionar como servidor push para los dispositivos administrados a través del protocolo móvil y para los dispositivos administrados por el Agente de red. Por ejemplo, se debe habilitar un servidor push si quiere poder forzar la sincronización de los dispositivos KasperskyOS con el Servidor de administración. Un servidor push tiene el mismo alcance de los dispositivos administrados que el punto de distribución en el que se habilitar el servidor push. Si tiene varios puntos de distribución asignados para el mismo grupo de administración, puede habilitar el servidor push en cada uno de los puntos de distribución. En este caso, el Servidor de administración equilibra la carga entre los puntos de distribución.

- **Puerto del servidor push**

  El número de puerto para el servidor push. Puede especificar el número de cualquier puerto que esté desocupado.

- En la sección **Alcance**, especifique el alcance al que el punto de distribución distribuirá las actualizaciones (grupos de administración y/o ubicación de red).

Para que un dispositivo pueda determinar su ubicación de red, debe tener un sistema operativo Windows. No se puede determinar la ubicación de red de dispositivos con otros sistemas operativos.

- Si el punto de distribución funciona en un equipo que no sea el Servidor de administración, en la sección **Origen de actualizaciones**, puede seleccionar una fuente de actualizaciones para el punto de distribución:

  - Origen de actualizaciones

    Seleccione un origen de actualizaciones para el punto de distribución:

    - Seleccione **Recuperar desde el Servidor de administración** para que el punto de distribución pueda recibir actualizaciones del Servidor de administración.
    - Seleccione **Usar una tarea de descarga de actualizaciones** para que el punto de distribución pueda utilizar una tarea para recibir las actualizaciones. A continuación, indique qué tarea *Descargar actualizaciones en los repositorios de los puntos de distribución* se usará:
      - Si la tarea que desea utilizar ya existe en el dispositivo, selecciónela en la lista.
      - Si la tarea aún no existe en el dispositivo, haga clic en el vínculo **Crear tarea** para crearla. Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente.

  - Descargar archivos diff

    Esta opción habilita la función de descarga de archivos diff.

    Esta opción está activada de forma predeterminada.

- Si sus puntos de distribución utilizan un servidor proxy al conectarse a Internet, en la subsección **Configuración de la conexión a Internet**, puede especificar la siguiente configuración:

  - Usar servidor proxy

    Si se selecciona esta casilla, en los campos de entrada puede configurar la conexión del servidor proxy.

    Esta casilla no está marcada de manera predeterminada.

  - Dirección del servidor proxy

    Dirección del servidor proxy.

  - Número de puerto

    Número de puerto que se utilizará para la conexión.

  - No usar el servidor proxy para direcciones locales

Si habilita esta opción, no se usará un servidor proxy para establecer conexión con los dispositivos de la red local.

Esta opción está deshabilitada de forma predeterminada.

- **Autenticación del servidor proxy**

  Si se selecciona esta casilla, en los campos de entrada se podrán especificar las credenciales para la autenticación del servidor proxy.

  Esta casilla no está marcada de manera predeterminada.

- **Nombre de usuario**

  Cuenta de usuario con la que se establece conexión con el servidor proxy.

- **Contraseña**

  Contraseña de la cuenta con la que se ejecutará la tarea.

- En la sección **Proxy de KSN**, puede configurar la aplicación para que utilice el punto de distribución para reenviar las solicitudes KSN desde los dispositivos administrados.

  - **Habilitar el proxy de KSN en el lado del punto de distribución**

    El servicio de proxy de KSN se ejecuta en el dispositivo que se utiliza como punto de distribución. Utilice esta función para redistribuir y optimizar el tráfico de la red.

    El punto de distribución enviará a Kaspersky las estadísticas de KSN que se enumeran en la declaración de Kaspersky Security Network. De forma predeterminada, la declaración de KSN se encuentra en %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

    Esta opción está deshabilitada de forma predeterminada. Esta opción solo se habilita si las opciones **Usar Servidor de administración como servidor proxy** y **Acepto utilizar Kaspersky Security Network** están habilitadas en la ventana de propiedades del Servidor de administración.

    Puede asignar un nodo de un clúster activo-pasivo a un punto de distribución y habilitar el servidor proxy de KSN en ese nodo.

  - **Transmitir las solicitudes para KSN al Servidor de administración**

    El punto de distribución envía las solicitudes KSN desde los dispositivos administrados al Servidor de administración.

    Esta opción está activada de forma predeterminada.

  - **Acceder a KSN Cloud/KPSN directamente a través de Internet**

El punto de distribución envía las solicitudes KSN desde los dispositivos administrados a KSN Cloud o a KPSN. Las solicitudes de KSN generadas en el punto de distribución mismo también se envían directamente a la nube de KSN Cloud o a KPSN.

Los puntos de distribución que tienen instalado el Agente de red versión 11 (o versiones anteriores) no pueden acceder a KPSN directamente. Si desea reconfigurar los puntos de distribución para enviar solicitudes de KSN a KPSN, habilite la opción **Reenviar solicitudes KSN al Servidor de administración** para cada punto de distribución.

Los puntos de distribución que tienen instalado el Agente de red versión 12 (o una posterior) pueden acceder a KPSN directamente.

- **No usar el servidor proxy configurado para conectarse a KPSN**

  Habilite esta opción, si tiene las configuraciones del servidor proxy configuradas en las propiedades del punto de distribución o en la directiva del Agente de red, pero su arquitectura de red requiere que use KPSN directamente. De lo contrario, las solicitudes de las aplicaciones administradas no podrán llegar a KPSN.

  Esta opción está disponible si selecciona la opción **Acceder a KSN Cloud/KPSN directamente a través de Internet**.

- **Puerto**

  El número del puerto de TCP que los dispositivos administrados utilizarán para conectarse al Servidor proxy de KSN. El número de puerto predeterminado es 13111.

- **Usar puerto UDP**

  Si necesita que los dispositivos administrados se conecten al servidor proxy de KSN a través de un puerto UDP, active la opción **Usar puerto UDP** y especifique un número de puerto UDP. Esta opción está activada de forma predeterminada.

- **Puerto UDP**

  El número del puerto de UDP que los dispositivos administrados utilizarán para conectarse al Servidor proxy de KSN. El puerto UDP predeterminado de conexión al servidor proxy de KSN es 15111.

- Si el punto de distribución funciona en un equipo que no sea el Servidor de administración, en la sección **Puerta de enlace de conexión**, puede configurar el punto de distribución para que actúe como una puerta de enlace para la conexión entre las instancias del Agente de red y el Servidor de administración:

  - **Puerta de enlace de conexión**

    Si no se puede establecer una conexión directa entre el Servidor de administración y los Agentes de red debido a la organización de su red, puede usar el punto de distribución para que actúe como la puerta de enlace de conexión entre el Servidor de administración y los Agentes de red.

    Habilite esta opción si necesita que el punto de distribución actúe como una puerta de enlace de conexión entre los Agentes de red y el Servidor de administración. Esta opción está deshabilitada de forma predeterminada.

- **Establecer la conexión a la puerta de enlace de conexión desde el Servidor de administración (si la puerta de enlace está en DMZ)**

  Si el Servidor de administración está ubicado fuera de la zona desmilitarizada (DMZ), en la red de área local, los Agentes de red instalados en dispositivos remotos no pueden conectarse al Servidor de administración. Puede usar un punto de distribución como puerta de enlace de conexión con conectividad inversa (el Servidor de administración establece una conexión con el punto de distribución).

  Habilite esta opción si necesita conectar el Servidor de administración a la puerta de enlace de conexión en DMZ.

- **Abrir puerto local para Kaspersky Security Center Web Console**

  Habilite esta opción si necesita la puerta de enlace de conexión en DMZ a fin de abrir un puerto para Web Console que está en DMZ o en Internet. Especifique el número de puerto que se usará para la conexión de Web Console al punto de distribución. El número de puerto predeterminado es 13299.

  Esta opción está disponible si habilita la opción **Establecer la conexión a la puerta de enlace de conexión desde el Servidor de administración (si la puerta de enlace está en DMZ)**.

Al conectar dispositivos móviles al Servidor de administración a través del punto de distribución que funciona como puerta de enlace de conexión, puede habilitar las siguientes opciones:

- **Abrir puerto para dispositivos móviles (solo autenticación SSL del Servidor de administración)**

  Habilite esta opción si necesita que la puerta de enlace de conexión abra un puerto para los dispositivos móviles y especifique el número de puerto que usarán los dispositivos móviles a fin de conectarse con el punto de distribución. El número de puerto predeterminado es 13292. El dispositivo móvil verificará el certificado del Servidor de administración. Al establecer la conexión, solo se autentica el Servidor de administración.

- **Abrir puerto para dispositivos móviles (autenticación SSL bidireccional)**

  Habilite esta opción si necesita una puerta de enlace de conexión a fin de abrir un puerto que se usará para la autenticación bidireccional del Servidor de administración y los dispositivos móviles. El dispositivo móvil verificará el certificado del Servidor de administración y el Servidor de administración verificará el certificado para dispositivos móviles. Especifique los siguientes parámetros:

  - Número de puerto que usarán los dispositivos móviles para conectarse con el punto de distribución. El número de puerto predeterminado es 13293.

  - Nombres de dominio DNS de la puerta de enlace de conexión que usarán los dispositivos móviles. Separe los nombres de dominio con comas. Los nombres de dominio especificados se incluirán en el certificado del punto de distribución. Si los nombres de dominio usados por los dispositivos móviles no coinciden con el nombre común en el certificado del punto de distribución, los dispositivos móviles no se conectan al punto de distribución.

    El nombre de dominio DNS predeterminado es el nombre FQDN de la puerta de enlace de conexión.

En ambos casos, los certificados se verifican solo cuando la sesión de TLS se estable en el punto de distribución. Los certificados no se reenvían para que los verifique el Servidor de administración. Al establecer una sesión de TLS con el dispositivo móvil, el punto de distribución utiliza el certificado del Servidor de administración para crear un túnel a fin de sincronizar el dispositivo móvil y el Servidor de administración. Si abre el puerto para la autenticación bidireccional de SSL, la única forma de distribuir el certificado para dispositivos móviles es a través de un paquete de instalación.

- Configure los sondeos de Active Directory, dominios de Windows e intervalos IP que realizará el punto de distribución:

  - Dominios de Windows

    Puede habilitar y programar el descubrimiento de dispositivos en los dominios de Windows.

  - Controladores de dominio

    Puede habilitar y programar el mecanismo de sondeo de red para Active Directory.

    Si utiliza un punto de distribución de Windows, puede seleccionar una de las siguientes opciones:

    - **Sondear el dominio actual de Active Directory**.
    - **Sondear el bosque de dominio de Active Directory**.
    - **Sondear solo los dominios de Active Directory seleccionados**. Si selecciona esta opción, agregue uno o más dominios de Active Directory a la lista.

    Si utiliza un punto de distribución de Linux con la versión 15 del Agente de red instalada, puede sondear solo los dominios de Active Directory para los cuales especifique la dirección y las credenciales de usuario. El sondeo del dominio de Active Directory actual y el bosque de dominios de Active Directory no está disponibles.

    Puede habilitar el descubrimiento de dispositivos para los controladores de dominio.

    Si selecciona la opción **Habilitar el sondeo de controladores de dominio**, puede seleccionar controladores de dominio para el sondeo y también especificar el programa de sondeo para ellos.

    Si utiliza un punto de distribución de Linux, en la sección **Sondear dominios específicos**, haga clic en **Agregar** y luego especifique la dirección y las credenciales de usuario del controlador de dominio.

    Si utiliza un punto de distribución de Windows, puede seleccionar una de las siguientes opciones:

    - **Sondear dominio actual**
    - **Sondear bosque de dominio entero**
    - **Sondear dominios específicos**

  - Intervalos IP

Puede habilitar el descubrimiento de dispositivos en intervalos IPv4 y en redes IPv6.

Tras habilitar la opción **Habilitar sondeo de intervalos**, podrá agregar los intervalos que se sondearán y definir una programación para los sondeos. Puede agregar rangos de IP a la lista de rangos analizados.

Si habilita la opción **Usar Zeroconf para el sondeo de redes IPv6**, el punto de distribución sondeará la red IPv6 automáticamente utilizando Zeroconf, una *tecnología para crear redes sin configuración*. En ese caso, el punto de distribución sondeará la red completa; el sondeo no estará limitado a los intervalos IP que especifique. La opción **Usar Zeroconf para el sondeo de redes IPv6** está disponible si el punto de distribución ejecuta Linux. Para usar el sondeo de Zeroconf IPv6, debe instalar la utilidad avahi-browse en el punto de distribución.

- En la sección **Avanzado**, especifique la carpeta en la que el punto de distribución guardará los datos distribuidos:
  - **Usar carpeta predeterminada**

    Si selecciona esta opción, la aplicación utilizará la carpeta de instalación del Agente de red en el punto de distribución.

  - **Usar carpeta especificada**

    Si selecciona esta opción, especifique la ruta a la carpeta en el campo que verá debajo. Puede usar una carpeta local del punto de distribución o una carpeta de otro dispositivo conectado a la red corporativa.

    La cuenta de usuario que se utilice para ejecutar el Agente de red en el punto de distribución deberá tener acceso de lectura y escritura a la carpeta especificada.

10. Haga clic en el botón **Aceptar**.

    El dispositivo seleccionado se designa como punto de distribución.

## Modificar la lista de puntos de distribución para un grupo de administración

Puede ver la lista de puntos de distribución asignados a un grupo de administración y, si necesita agregar o quitar puntos de distribución, modificarla.

*Para ver y modificar la lista de puntos de distribución asignados a un grupo de administración:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.
2. En el campo **Ruta actual** ubicado sobre la lista de dispositivos administrados, haga clic en el vínculo de la ruta.
3. En el panel del lado izquierdo que se abre, seleccione el grupo de administración cuyos puntos de distribución asignados desee ver.

   Se habilitará el elemento **Puntos de distribución** en el menú.
4. En el menú principal, vaya a **Activos (dispositivos)** → **Puntos de distribución**.

5. Para agregar nuevos puntos de distribución para el grupo de administración, haga clic en el botón **Asignar** ubicado sobre la lista de dispositivos administrados y seleccione los dispositivos en el panel que se abrirá.

6. Para eliminar los puntos de distribución asignados, seleccione dispositivos de la lista y haga clic en el botón **Desasignar**.

Dependiendo de sus acciones, se agregarán nuevos puntos de distribución a la lista o se quitarán puntos de distribución de la lista.

## Sincronización forzada

Aunque Kaspersky Security Center sincroniza el estado, la configuración, las tareas y las directivas automáticamente para los dispositivos administrados, en algunos casos puede que desee ejecutar la sincronización para un dispositivo específico de manera forzada. Puede ejecutar una sincronización forzada para los siguientes dispositivos:

- Dispositivos que tienen el Agente de red instalado
- Dispositivos que ejecuten KasperskyOS

  Antes de ejecutar la sincronización forzada para un dispositivo KasperskyOS, asegúrese de que el dispositivo esté incluido en el alcance de un punto de distribución y de que haya un servidor push habilitado en el punto de distribución.
- Dispositivos iOS
- Dispositivos Android

  Antes de ejecutar una sincronización forzada para un dispositivo Android, debe configurar Firebase Cloud Messaging.

### Sincronizar un solo dispositivo

*Para forzar la sincronización entre el Servidor de administración y un dispositivo administrado:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.
2. Haga clic en el nombre del dispositivo que desee sincronizar con el Servidor de administración.

   Se abrirá una ventana de propiedades con la sección **General** seleccionada.
3. Haga clic en el botón **Forzar sincronización**.

La aplicación sincronizará el dispositivo seleccionado con el Servidor de administración.

## Sincronizar más de un dispositivo

*Para forzar la sincronización entre el Servidor de administración y varios dispositivos administrados:*

1. Abra la lista de dispositivos de un grupo de administración o una selección de dispositivos:

   - En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados** y haga clic en el vínculo de la ruta que verá en el campo **Ruta actual** ubicado sobre la lista de dispositivos administrados. A continuación, seleccione el grupo de administración que contenga los dispositivos que desee sincronizar.

   - Genere una selección de dispositivos para ver la lista de dispositivos.

2. Active las casillas de verificación ubicadas junto a los dispositivos que desee sincronizar con el Servidor de administración.

3. Haga clic en el botón de los tres puntos ( ... ) ubicado sobre la lista de dispositivos administrados. A continuación, haga clic en el botón **Forzar sincronización**.

   La aplicación sincronizará los dispositivos seleccionados con el Servidor de administración.

4. En la lista de dispositivos, verifique a qué hora se registró la última conexión de los dispositivos seleccionados con el Servidor de administración. La hora debería haber cambiado a la actual. Si la hora no cambió, haga clic en el botón **Actualizar** para actualizar el contenido de la página.

Los dispositivos seleccionados quedan sincronizados con el Servidor de administración.

## Ver la hora de entrega de una directiva

Después de cambiar una directiva para una aplicación de Kaspersky en el Servidor de administración, el administrador puede verificar si la directiva modificada se ha entregado a un dispositivo administrado específico. Una directiva se puede entregar durante una sincronización regular o una sincronización forzada.

*Para ver la fecha y la hora en que la directiva de una aplicación se entregó a un dispositivo administrado:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.

2. Haga clic en el nombre del dispositivo que desee sincronizar con el Servidor de administración.

   Se abrirá una ventana de propiedades con la sección **General** seleccionada.

3. Seleccione la pestaña **Aplicaciones**.

4. Seleccione la aplicación para la que desee ver la fecha de sincronización de la directiva.

   Se abrirá la ventana de la directiva de la aplicación. La sección **General** estará seleccionada. Allí encontrará la fecha y la hora en que se entregó la directiva.

## Habilitación de un servidor push

En Kaspersky Security Center, un punto de distribución puede funcionar como servidor push para los dispositivos administrados a través del protocolo móvil y para los dispositivos administrados por el Agente de red. Por ejemplo, se debe habilitar un servidor push si quiere poder forzar la sincronización de los dispositivos KasperskyOS con el Servidor de administración. Un servidor push tiene el mismo alcance de los dispositivos administrados que el punto de distribución en el que se habilitar el servidor push. Si tiene varios puntos de distribución asignados para el mismo grupo de administración, puede habilitar el servidor push en cada uno de los puntos de distribución. En este caso, el Servidor de administración equilibra la carga entre los puntos de distribución.

Puede utilizar puntos de distribución como servidores push para asegurarse de que haya una conectividad continua entre un dispositivo administrado y el Servidor de administración. Se necesita conectividad continua para algunas operaciones, como ejecutar y detener tareas locales, recibir estadísticas para una aplicación administrada o crear un túnel. Si utiliza un punto de distribución como servidor push, no es necesario utilizar la opción **No desconectar del Servidor de administración** en dispositivos administrados ni enviar paquetes al puerto UDP del Agente de red.

Un servidor push soporta la carga de hasta 50 000 conexiones simultáneas.

*Para habilitar un servidor push en un punto de distribución:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Puntos de distribución**.

3. Haga clic en el nombre del punto de distribución en el que desea habilitar el servidor push.

   Se abre la ventana de propiedades del punto de distribución.

4. En la sección **General**, habilite la opción **Ejecutar servidor push**.

5. En el campo **Puerto del servidor push**, escriba el número de puerto. Puede especificar el número de cualquier puerto desocupado.

6. En el campo **Dirección para hosts remotos**, especifique la dirección IP o el nombre del dispositivo del punto de distribución.

7. Haga clic en el botón **Aceptar**.

El servidor push está habilitado en el punto de distribución seleccionado.

# Administración de aplicaciones de terceros en dispositivos cliente

En esta sección, se describen las características de Kaspersky Security Center relacionadas con la administración de aplicaciones de terceros instaladas en dispositivos cliente.

# Instalación de actualizaciones para software de terceros

Kaspersky Security Center le permite administrar actualizaciones de software de terceros instaladas en dispositivos administrados y reparar vulnerabilidades en aplicaciones de Microsoft y productos de otros fabricantes de software, mediante la instalación de actualizaciones requeridas.

Kaspersky Security Center busca actualizaciones a través de la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Cuando se completa esta tarea, el Servidor de administración recibe listas en las que se detallan las vulnerabilidades detectadas y las actualizaciones requeridas para el software de terceros con el que cuentan los dispositivos indicados en las propiedades de la tarea. Tras ver la información de las actualizaciones disponibles, puede instalarlas en los dispositivos.

Para actualizar algunas aplicaciones, Kaspersky Security Center elimina la versión anterior de la aplicación e instala la versión nueva.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedírsele al usuario que la cierre.

Por seguridad, cada actualización de software de terceros que se instala con la función Administración de vulnerabilidades y parches se somete a un análisis antimalware automático con las tecnologías de Kaspersky Estas tecnologías revisan automáticamente los archivos utilizando técnicas de análisis antivirus, análisis estático, análisis dinámico, análisis de comportamiento en un entorno de pruebas y aprendizaje automático, entre otras.

Los expertos de Kaspersky no realizan análisis manuales de las actualizaciones de software de terceros que puedan instalarse mediante la función Administración de vulnerabilidades y parches. Tampoco buscan vulnerabilidades (conocidas o desconocidas) o funciones no documentadas en las actualizaciones ni las analizan de modos que no se hayan indicado en el párrafo anterior.

### Tareas para la instalación de actualizaciones de software de terceros

Una vez que los metadatos de las actualizaciones de software de terceros se descargan al repositorio, puede usar las siguientes tareas para instalar las actualizaciones en los dispositivos cliente:

- La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*

  La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se utiliza para instalar actualizaciones para aplicaciones de Microsoft (incluidas las actualizaciones que proporciona el servicio Windows Update) y actualizaciones para software de otros proveedores. Tenga en cuenta que esta tarea se puede crear únicamente si se cuenta con una licencia para la función Administración de vulnerabilidades y parches.

  Cuando se completa esta tarea, las actualizaciones se instalan en los dispositivos administrados automáticamente. Cuando se descargan metadatos de nuevas actualizaciones en el repositorio del Servidor de administración, Kaspersky Security Center verifica si las actualizaciones cumplen con los criterios especificados en las reglas de actualización. Las actualizaciones nuevas que cumplen con los criterios se descargan e instalan en forma automática cuando la tarea se ejecuta nuevamente.

- La tarea *Instalar actualizaciones de Windows Update*

  La tarea *Instalar actualizaciones de Windows Update* no requiere licencia, pero solo se la puede utilizar para instalar actualizaciones de Windows Update.

  Cuando se completa esta tarea, se instalan únicamente las actualizaciones especificadas en sus propiedades. En el futuro, si desea instalar nuevas actualizaciones descargadas en el repositorio del Servidor de administración, deberá agregar las actualizaciones necesarias a la lista de actualizaciones en la tarea actual o crear una nueva tarea Instalar actualizaciones de Windows Update.

### Uso del Servidor de administración como servidor WSUS

El servicio de Windows Update proporciona información de las actualizaciones disponibles para Microsoft Windows. Se puede usar el Servidor de administración como el servidor de Windows Server Update Services (WSUS). Para usar el Servidor de administración como servidor de WSUS, debe crear la tarea Realizar la sincronización de Windows Update y seleccionar la opción **Utilizar el Servidor de administración como servidor WSUS** en la directiva del Agente de red. Una vez que haya configurado la sincronización de datos con Windows Update, el Servidor de administración proporciona actualizaciones para los servicios de Windows Update en dispositivos, en modo centralizado y con la frecuencia definida.

## Procedimiento: Actualización de software de terceros

En esta sección, se describe un escenario para actualizar el software de terceros instalado en los dispositivos cliente. El término "software de terceros" comprende aplicaciones desarrolladas por Microsoft y por otros proveedores de software. Las actualizaciones para las aplicaciones de Microsoft se obtienen a través del servicio Windows Update.

### Requisitos previos

El Servidor de administración debe tener conexión a Internet para instalar actualizaciones de software de terceros que no sean software de Microsoft.

De forma predeterminada, el Servidor de administración no requiere conexión a Internet para instalar las actualizaciones de software de Microsoft en los dispositivos administrados. Los dispositivos administrados pueden descargar las actualizaciones de software de Microsoft directamente de los servidores de Microsoft Update, por ejemplo, o de un servidor Windows Server que esté desplegado en la red de la organización y que tenga Windows Server Update Services (WSUS) habilitado. El Servidor de administración debe estar conectado a Internet cuando utilice el Servidor de administración como servidor WSUS.

## Etapas

El proceso para actualizar aplicaciones de terceros se divide en etapas:

1. **Buscar las actualizaciones requeridas**

   Para buscar las actualizaciones que se requieren para el software de terceros de los dispositivos administrados, ejecute la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Cuando se completa esta tarea, Kaspersky Security Center recibe las listas de vulnerabilidades detectadas y las actualizaciones necesarias para el software de terceros instalado en los dispositivos que especificó en las propiedades de la tarea.

   La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea automáticamente al utilizar el asistente de inicio rápido del Servidor de administración. Si no ejecutó el asistente de inicio rápido, hágalo ahora o cree la tarea.

   Instrucciones:

   - Consola de administración: Análisis de aplicaciones en busca de vulnerabilidades, Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas
   - Kaspersky Security Center Web Console: Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas, Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

2. **Analizar la lista de actualizaciones encontradas**

   Abra la lista **Actualizaciones de software** y decida qué actualizaciones se instalarán. Para obtener información detallada sobre una actualización, haga clic en el nombre de la misma en la lista. Para cada actualización de la lista, también puede ver las estadísticas sobre su instalación en los dispositivos cliente.

   Instrucciones:

   - Consola de administración: Ver información sobre las actualizaciones disponibles
   - Kaspersky Security Center Web Console: Ver información sobre las actualizaciones disponibles para el software de terceros

3. **Configurar la instalación de las actualizaciones**

   Una vez que Kaspersky Security Center cuente con la lista de actualizaciones para el software de terceros, utilice una de dos tareas para instalar las actualizaciones en los dispositivos cliente: la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Instalar actualizaciones de Windows Update*. Cree una de estas tareas. Puede crearlas desde la pestaña **Tareas** o a través de la lista **Actualizaciones de software**.

   La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se utiliza para instalar actualizaciones para aplicaciones de Microsoft (incluidas las actualizaciones que proporciona el servicio Windows Update) y actualizaciones para software de otros proveedores. Tenga en cuenta que esta tarea se puede crear únicamente si se cuenta con una licencia para la función Administración de vulnerabilidades y parches.

   La tarea *Instalar actualizaciones de Windows Update* no requiere licencia, pero solo se la puede utilizar para instalar actualizaciones de Windows Update.

   Para instalar algunas actualizaciones de software, deberá aceptar el Contrato de licencia de usuario final (EULA) para el software de instalación. Si rechaza el EULA, no se instalará la actualización de software correspondiente.

Puede iniciar una tarea de instalación de actualizaciones según una programación. Si elige configurar una programación, asegúrese de que la tarea de instalación de actualizaciones se ejecute luego de que finalice la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

Instrucciones:

- Consola de administración: Reparación de vulnerabilidades en las aplicaciones, Ver información sobre las actualizaciones disponibles
- Kaspersky Security Center Web Console: Creación de la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades, Creación de la tarea Instalar actualizaciones de Windows Update, Ver información sobre las actualizaciones disponibles para el software de terceros

4 **Programar las tareas**

Para asegurarse de que la lista de actualizaciones siempre esté actualizada, defina una programación que haga que la tarea *Buscar vulnerabilidades y actualizaciones requeridas* se ejecute automáticamente de tanto en tanto. De manera predeterminada, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* está configurada para iniciarse de forma manual.

Si ha creado la tarea *Instalar actualizaciones necesarias y reparar vulnerabilidades*, puede programarla para que se ejecute con igual o menor frecuencia que la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Al programar la tarea *Instalar actualizaciones de Windows Update*, tenga en cuenta que deberá definir la lista de actualizaciones cada vez que la tarea vaya a iniciarse.

Cuando programe las tareas, asegúrese de que la tarea de instalación de actualizaciones se inicie después de que la tarea *Buscar vulnerabilidades y actualizaciones requeridas* haya finalizado.

5 **Aprobar y rechazar actualizaciones de software (opcional)**

Si creó la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades, puede especificar reglas para la instalación de actualizaciones en las propiedades de la tarea. Si creó la tarea Instalar actualizaciones de Windows Update, omita este paso.

Para cada regla, puede definir las actualizaciones que se instalarán según el estado de la actualización (*Sin definir*, *Aprobada* o *Rechazada*). Si crea una tarea específica para sus servidores, por ejemplo, podría definir una regla que únicamente permita la instalación de actualizaciones que provengan de Windows Update y que tengan el estado *Aprobada*. Tras ello, podría asignar manualmente el estado *Aprobada* a las actualizaciones que desee instalar. Las actualizaciones de Windows Update que tengan el estado *Sin definir* o el estado *Rechazada* no se instalarán en los servidores especificados en la tarea.

Puede usar el estado *Aprobada* para administrar la instalación de un número modesto de actualizaciones. Cuando necesite instalar muchas actualizaciones, utilice, en cambio, las reglas que puede configurar en la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Asigne el estado *Aprobada* únicamente a las actualizaciones que no cumplan con los criterios indicados en las reglas. Aprobar un gran número de actualizaciones en forma manual afecta el rendimiento del Servidor de administración y puede, incluso, hacer que se sobrecargue.

De forma predeterminada, las actualizaciones de software descargadas tienen el estado *Sin definir*. Puede cambiar el estado a *Aprobada* o *Rechazada* en la lista **Actualizaciones de software** (**Operaciones** → **Administración de parches** → **Actualizaciones de software**).

Instrucciones:

- Consola de administración: Aprobar y rechazar actualizaciones de software
- Kaspersky Security Center Web Console: Aprobar y rechazar actualizaciones de software de terceros

6 **Configurar el Servidor de administración para que funcione como servidor de Windows Server Update Services (WSUS) (opcional)**

De manera predeterminada, las actualizaciones de Windows Update se descargan en los dispositivos administrados desde los servidores de Microsoft. Puede cambiar esta configuración para utilizar el Servidor de administración como servidor de WSUS. En este caso, el Servidor de administración sincroniza los datos de la actualización con Windows Update en la frecuencia especificada y proporciona actualizaciones en modo centralizado a Windows Update en los dispositivos en red.

Para utilizar el Servidor de administración como servidor WSUS, cree la tarea "Sincronización con Windows Update" y marque la casilla **Usar el Servidor de administración como servidor WSUS** en la directiva del Agente de red.

Instrucciones:

- Consola de administración: Sincronización de las actualizaciones de Windows Update con el Servidor de administración, Configuración de actualizaciones de Windows en una directiva del Agente de red
- Kaspersky Security Center Web Console: Creación de la tarea de sincronización con Windows Update

7. **Ejecutar una tarea de instalación de actualizaciones**

   Inicie la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Instalar actualizaciones de Windows Update*. Al hacerlo, se descargarán las actualizaciones y se las instalará en los dispositivos administrados. Cuando se complete la tarea ejecutada, verifique que su estado en la lista de tareas sea *Completada correctamente*.

8. **Crear el informe sobre los resultados de la instalación de actualizaciones de software de terceros (opcional)**

   Para ver estadísticas detalladas sobre la instalación de las actualizaciones, genere el **Informe sobre los resultados de la instalación de actualizaciones de software de terceros**.

   Instrucciones:

   - Consola de administración: Crear y ver un informe
   - Kaspersky Security Center Web Console: Generar y ver un informe

## Resultados

Si creó y configuró la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, las actualizaciones se instalarán automáticamente en los dispositivos administrados. Cuando se descargan nuevas actualizaciones en el repositorio del Servidor de administración, Kaspersky Security Center verifica si cumplen con los criterios especificados en las reglas de actualización. Todas las actualizaciones nuevas que cumplan con los criterios se instalarán automáticamente la próxima vez que se ejecute la tarea.

Si creó la tarea *Instalar actualizaciones de Windows Update*, solo se instalarán las actualizaciones especificadas en las propiedades de la tarea *Instalar actualizaciones de Windows Update*. En el futuro, si desea instalar nuevas actualizaciones descargadas en el repositorio del Servidor de administración, deberá agregar las actualizaciones necesarias a la lista de actualizaciones de la tarea existente o deberá crear una nueva tarea *Instalar actualizaciones de Windows Update*.

# Instalación de actualizaciones para software de terceros

Para instalar actualizaciones para software de terceros en sus dispositivos administrados, debe crear y ejecutar alguna de las siguientes tareas:

- *Instalar actualizaciones requeridas y reparar vulnerabilidades*

  La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se puede crear únicamente si tiene la licencia para la función Administración de vulnerabilidades y parches. Utilice esta tarea para instalar actualizaciones de Windows Update proporcionadas por Microsoft o actualizaciones para productos de otros proveedores.

- *Instalar actualizaciones de Windows Update*

  Puede usar la tarea *Instalar actualizaciones de Windows Update* para instalar solo actualizaciones de Windows Update.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedirle al usuario que la cierre.

Como alternativa, para crear una tarea que instale las actualizaciones requeridas, puede optar por estos métodos:

- Abra la lista de actualizaciones y elija las actualizaciones que se deban instalar.

  Como resultado, se creará una nueva tarea para instalar las actualizaciones seleccionadas. Si lo prefiere, puede agregar las actualizaciones seleccionadas a una tarea existente.

- Utilice el Asistente de instalación de actualizaciones.

  Para usar el Asistente de instalación de actualizaciones, debe tener una licencia de Administración de vulnerabilidades y parches.

  El asistente simplifica la creación y configuración de una tarea de instalación de actualizaciones, y permite eliminar la creación de tareas redundantes que contengan las mismas actualizaciones a instalar.

## Instalación de actualizaciones de software de terceros desde la lista de actualizaciones

*Para instalar actualizaciones de software de terceros desde la lista de actualizaciones:*

1. Abra una de las listas de actualizaciones:

   - Para abrir la lista de actualizaciones general, en el menú principal, vaya a **Operaciones → Administración de parches → Actualizaciones de software**.
   - Para abrir la lista de actualizaciones de un dispositivo administrado, en el menú principal, vaya a **Activos (dispositivos) → Dispositivos administrados →** <nombre del dispositivo> **→ Avanzado → Actualizaciones disponibles**.
   - Para abrir la lista de actualizaciones de una aplicación específica, en el menú principal vaya a **Operaciones → Aplicaciones de terceros → Registro de aplicaciones →** <nombre de la aplicación> **→ Actualizaciones disponibles**.

   Se mostrará una lista con las actualizaciones disponibles.

2. Marque las casillas de verificación ubicadas junto a las actualizaciones que desee instalar.

3. Haga clic en el botón **Instalar actualizaciones**.

   Para instalar algunas actualizaciones de software, deberá aceptar el contrato de licencia de usuario final (EULA). Si rechaza el EULA, no se instalará la actualización de software correspondiente.

4. Seleccione una de las siguientes opciones:

   - **Nueva tarea**

     Se inicia el Asistente para crear nueva tarea. Si tiene la licencia de la Administración de vulnerabilidades y parches, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* estará preseleccionada. Si no tiene la licencia, la tarea *Instalar actualizaciones de Windows Update* está preseleccionada. Siga los pasos del asistente para completar la creación de la tarea.

   - **Instalar actualización (agregar regla a la tarea especificada)**

     Seleccione una tarea a la que desee agregar las actualizaciones seleccionadas. Si tiene la licencia de Administración de vulnerabilidades y parches, seleccione la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Una nueva regla para instalar las actualizaciones seleccionadas se agregará automáticamente a la tarea seleccionada. Si no tiene la licencia, seleccione la tarea *Instalar actualizaciones de Windows Update*. Las actualizaciones seleccionadas se agregarán a las propiedades de la tarea.

     Se abrirá la ventana de propiedades de la tarea. Haga clic en el botón **Guardar** para guardar los cambios.

   Si optó por crear una tarea, se la creará y se la agregará a la lista de tareas disponible en **Activos (dispositivos) → Tareas**. Si eligió agregar las actualizaciones a una tarea existente, se agregarán las actualizaciones a las propiedades de la tarea que haya seleccionado.

Para instalar las actualizaciones para el software de terceros, inicie la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Instalar actualizaciones de Windows Update*. Puede iniciar cualquiera de estas dos tareas de forma manual o, si lo prefiere, puede configurar una programación en las propiedades de la tarea que desee iniciar. Si elige configurar una programación, asegúrese de que la tarea de instalación de actualizaciones se ejecute luego de que finalice la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

# Instalación de actualizaciones de software de terceros mediante el Asistente de instalación de actualizaciones

Para usar el Asistente de instalación de actualizaciones, debe tener una licencia de Administración de vulnerabilidades y parches.

*Para crear una tarea para instalar actualizaciones de software de terceros con el Asistente de instalación de actualizaciones:*

1. En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Actualizaciones de software**.

   Se mostrará una lista con las actualizaciones disponibles.

2. Marque la casilla ubicada junto a la actualización que desee instalar.

3. Haga clic en el botón **Ejecutar el Asistente de instalación de actualizaciones**.

   Se iniciará el Asistente de instalación de actualizaciones. En la página **Seleccione una tarea de instalación de actualizaciones**, verá una lista con todas las tareas existentes de los siguientes tipos:

   - *Instalar actualizaciones requeridas y reparar vulnerabilidades*
   - *Instalar actualizaciones de Windows Update*
   - *Reparar vulnerabilidades*

   No puede modificar las tareas de los dos últimos tipos para instalar nuevas actualizaciones. Para instalar nuevas actualizaciones, solo puede utilizar las tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

4. Si desea que el asistente solamente le muestre las tareas que permitan instalar la actualización seleccionada, habilite la opción **Mostrar solo las tareas que permitan instalar esta actualización**.

5. Elija lo que desea hacer:

   - Para iniciar una tarea, marque la casilla ubicada junto al nombre de la tarea en cuestión y haga clic en el botón **Iniciar**.

   - Para agregar una nueva regla a una tarea existente, haga lo siguiente:

     a. Marque la casilla ubicada junto al nombre de la tarea pertinente y haga clic en el botón **Agregar regla**.

     b. En la página que se abrirá, configure la nueva regla:

     - **Regla de instalación para actualizaciones de este nivel de importancia**

       Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

       Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al nivel de gravedad de la actualización seleccionada. Los niveles posibles son **Medio**, **Alto** y **Crítico**. Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

       Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

       Esta opción está deshabilitada de forma predeterminada.

     - **Regla de instalación para actualizaciones de este nivel de importancia conforme a MSRC**

       Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

       Si esta opción (que solo está disponible para actualizaciones de Windows Update) está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que el Centro de respuestas de seguridad de Microsoft (MSRC) haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

       Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

       Esta opción está deshabilitada de forma predeterminada.

     - **Regla de instalación para actualizaciones de este proveedor**

       Esta opción solo está disponible para actualizaciones de aplicaciones de terceros. Kaspersky Security Center instala solo las actualizaciones relacionadas con las aplicaciones realizadas por el mismo proveedor que la actualización seleccionada. No se instalarán actualizaciones rechazadas ni actualizaciones para software de otros proveedores.

       Esta opción está deshabilitada de forma predeterminada.

     - **Regla de instalación para actualizaciones del tipo**

- **Regla de instalación para la actualización seleccionada**

- Aprobar actualizaciones seleccionadas

  Se aprobará la instalación de la actualización seleccionada. Habilite esta opción si ha aplicado reglas de instalación de actualizaciones que solo permitan instalar actualizaciones aprobadas.

  Esta opción está deshabilitada de forma predeterminada.

- Instalar automáticamente todas las actualizaciones de software que antecedan a las seleccionadas y se requieran para instalarlas

  Mantenga habilitada esta opción si está de acuerdo en que, para instalar las actualizaciones seleccionadas, se instalen versiones intermedias de las aplicaciones.

  Si deshabilita esta opción, se instalarán únicamente las versiones de las aplicaciones que haya seleccionado. Deshabilite esta opción si quiere que las aplicaciones se actualicen en forma directa, sin que se trate de instalar versiones intermedias. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

  A modo de ejemplo, imagine que un dispositivo tiene instalada la versión 3 de una aplicación. Quiere actualizar esa versión a la 5, pero la versión 5 solo se puede instalar sobre la versión 4. Si esta opción está habilitada, el software instalará primero la versión 4 y luego la versión 5. Si esta opción está deshabilitada, el software no podrá actualizar la aplicación.

  Esta opción está activada de forma predeterminada.

c. Haga clic en el botón **Agregar**.

- Para crear una tarea:

  a. Haga clic en el botón **Nueva tarea**.

  b. En la página que se abrirá, configure la nueva regla:

  - Regla de instalación para actualizaciones de este nivel de importancia

    Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

    Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al nivel de gravedad de la actualización seleccionada. Los niveles posibles son **Medio**, **Alto** y **Crítico**. Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

    Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

    Esta opción está deshabilitada de forma predeterminada.

  - Regla de instalación para actualizaciones de este nivel de importancia conforme a MSRC

Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

Si esta opción (que solo está disponible para actualizaciones de Windows Update) está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que el Centro de respuestas de seguridad de Microsoft (MSRC) haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

Esta opción está deshabilitada de forma predeterminada.

- Regla de instalación para actualizaciones de este proveedor

  Esta opción solo está disponible para actualizaciones de aplicaciones de terceros. Kaspersky Security Center instala solo las actualizaciones relacionadas con las aplicaciones realizadas por el mismo proveedor que la actualización seleccionada. No se instalarán actualizaciones rechazadas ni actualizaciones para software de otros proveedores.

  Esta opción está deshabilitada de forma predeterminada.

- **Regla de instalación para actualizaciones del tipo**

- **Regla de instalación para la actualización seleccionada**

- Aprobar actualizaciones seleccionadas

  Se aprobará la instalación de la actualización seleccionada. Habilite esta opción si ha aplicado reglas de instalación de actualizaciones que solo permitan instalar actualizaciones aprobadas.

  Esta opción está deshabilitada de forma predeterminada.

- Instalar automáticamente todas las actualizaciones de software que antecedan a las seleccionadas y se requieran para instalarlas

  Mantenga habilitada esta opción si está de acuerdo en que, para instalar las actualizaciones seleccionadas, se instalen versiones intermedias de las aplicaciones.

  Si deshabilita esta opción, se instalarán únicamente las versiones de las aplicaciones que haya seleccionado. Deshabilite esta opción si quiere que las aplicaciones se actualicen en forma directa, sin que se trate de instalar versiones intermedias. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

  A modo de ejemplo, imagine que un dispositivo tiene instalada la versión 3 de una aplicación. Quiere actualizar esa versión a la 5, pero la versión 5 solo se puede instalar sobre la versión 4. Si esta opción está habilitada, el software instalará primero la versión 4 y luego la versión 5. Si esta opción está deshabilitada, el software no podrá actualizar la aplicación.

  Esta opción está activada de forma predeterminada.

c. Haga clic en el botón **Agregar**.

Si eligió iniciar una tarea, puede cerrar el asistente. La tarea se completará en segundo plano. No se requieren más acciones.

Si optó por agregar una regla a una tarea existente, se abrirá la ventana de propiedades de la tarea. Encontrará la nueva regla en las propiedades de la tarea. Si lo desea, vea y modifique la regla u otros ajustes de la tarea. Haga clic en el botón **Guardar** para guardar los cambios.

Si eligió crear una tarea, continúe creándola en el Asistente para crear nueva tarea. La regla agregada en el Asistente de instalación de actualizaciones se mostrará en el Asistente para crear nueva tarea. Cuando llegue al final del asistente, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se agregará a la lista de tareas.

## Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas

Mediante la tarea Buscar vulnerabilidades y actualizaciones requeridas, Kaspersky Security Center recibe las listas de las vulnerabilidades detectadas y las actualizaciones necesarias para el software de terceros instalado en los dispositivos administrados.

La tarea Buscar vulnerabilidades y actualizaciones requeridas se crea automáticamente cuando se ejecuta el asistente de inicio rápido. Si no ha ejecutado este asistente, puede crear la tarea de forma manual.

*Para crear una tarea del tipo Buscar vulnerabilidades y actualizaciones requeridas:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.
3. Para la aplicación de Kaspersky Security Center, seleccione el tipo de tarea **Buscar vulnerabilidades y actualizaciones requeridas**.
4. Escriba un nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).
5. Seleccione los dispositivos a los que se asignará la tarea.
6. Si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.
7. Haga clic en el botón **Crear**.

   Se crea la tarea y se la agrega a la lista de tareas.
8. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.
9. En la ventana de propiedades de la tarea, configure los ajustes generales de la tarea.

10. En la pestaña **Configuración de la aplicación**, defina los siguientes ajustes:

- **Buscar vulnerabilidades y actualizaciones catalogadas por Microsoft**

  Al buscar vulnerabilidades y actualizaciones, Kaspersky Security Center utiliza la información sobre las actualizaciones de Microsoft aplicables desde la fuente de actualizaciones de Microsoft, las cuales están disponibles en este momento.

  Podría deshabilitar esta opción si, por ejemplo, ha creado tareas diferentes (con configuraciones diferentes) para las actualizaciones de Microsoft y para las actualizaciones de aplicaciones de terceros.

  Esta opción está activada de forma predeterminada.

  La información sobre las actualizaciones opcionales de Microsoft Windows no se envía al Servidor de administración.

- **Conectarse al servidor de actualizaciones para actualizar los datos**

El Agente de Windows Update del dispositivo administrado se conectará al origen de actualizaciones de Microsoft. Los siguientes servidores pueden actuar como orígenes de actualizaciones de Microsoft:

- Servidor de administración de Kaspersky Security Center (consulte la configuración de la directiva del Agente de red)
- Un servidor Windows Server con Microsoft Windows Server Update Services (WSUS) que se encuentre instalado en la red de su organización
- Los servidores de actualizaciones de Microsoft

Cuando esta opción está habilitada, el Agente de Windows Update del dispositivo administrado se conecta al origen de actualizaciones de Microsoft para obtener información actualizada sobre las actualizaciones de Microsoft Windows aplicables.

Cuando esta opción está deshabilitada, el Agente de actualización de Windows del dispositivo administrado usa la información sobre las actualizaciones de Microsoft Windows aplicables que el origen de actualizaciones brindó en un momento anterior.

Conectarse al origen de actualizaciones de Microsoft puede consumir muchos recursos. Podría deshabilitar esta opción si ha configurado un esquema de conexión periódica a este origen en otra tarea o en la sección **Actualizaciones y vulnerabilidades de software** de las propiedades de la directiva del Agente de red. Si no quiere deshabilitar esta opción, para intentar que el Servidor de administración no se sobrecargue, modifique la programación de la tarea para que se la inicie en un punto aleatorio de un intervalo de 360 minutos.

Esta opción está activada de forma predeterminada.

El modo de obtener las actualizaciones deriva de combinar las siguientes opciones de configuración de la directiva del Agente de red:

- El Agente de Windows Update en un dispositivo administrado se conecta al Servidor de actualizaciones para obtener actualizaciones solo si la opción **Conectarse al servidor de actualizaciones para actualizar los datos** está activada en las propiedades de la tarea *Buscar vulnerabilidades y actualizaciones requeridas* y la opción de **Modo de búsqueda de Windows Update** está configurada como **Activo** en la configuración de la directiva del Agente de red.
- Si no necesita el Agente de red para iniciar una conexión al origen de actualizaciones de Microsoft Windows ni para descargar actualizaciones al realizar la tarea *Análisis de vulnerabilidades*, puede seleccionar la opción **Pasivo** en **Modo de búsqueda de Windows Update**, pero la opción **Conectarse al servidor de actualizaciones para actualizar los datos** debe permanecer habilitada. Así podrá ahorrar recursos y usar las actualizaciones de Windows antes recibidas para analizar las vulnerabilidades. Puede usar el modo pasivo si configura la recepción de actualizaciones de Microsoft Windows de otra manera. Si la recepción de actualizaciones de Microsoft Windows no está configurada de otra manera, no seleccione la opción **Pasivo** en **Modo de búsqueda de Windows Update** porque, en este caso, nunca recibirá información sobre las actualizaciones.
- Independientemente del estado de la opción **Conectarse al servidor de actualizaciones para actualizar los datos** (habilitado o deshabilitado), si se selecciona la opción **Modo de búsqueda de Windows Update** en **Deshabilitado**, Kaspersky Security Center no solicita ninguna información sobre actualizaciones.

- Buscar vulnerabilidades y actualizaciones catalogadas por Kaspersky para software de terceros

Si esta opción está habilitada, Kaspersky Security Center busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft) en el Registro de Windows y en las carpetas especificadas en **Especifique las rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**. Kaspersky determina el alcance de la lista de aplicaciones de terceros compatibles.

Si esta opción está deshabilitada, Kaspersky Security Center no busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros. Puede que quiera deshabilitar esta opción si utiliza tareas diferentes, con configuraciones diferentes, para las actualizaciones de Microsoft Windows y para las actualizaciones de aplicaciones de terceros.

Esta opción está activada de forma predeterminada.

- **Especifique las rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**

  Carpetas en las que Kaspersky Security Center buscará aplicaciones de terceros que requieran la instalación de actualizaciones o que tengan vulnerabilidades que deban repararse. Puede utilizar variables del sistema.

  Especifique las carpetas en las que se instalan las aplicaciones. De forma predeterminada, la lista contiene carpetas del sistema en las que se instalan la mayoría de las aplicaciones.

- **Habilitar diagnóstico avanzado**

  Si esta función está habilitada, el Agente de red escribe archivos de seguimiento, incluso si la escritura de archivos de seguimiento está deshabilitada para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center. Los datos de seguimiento se guardan en dos archivos sucesivamente; el tamaño total de ambos archivos está determinado por el valor de la opción **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando los archivos alcanzan su límite de tamaño, el Agente de red comienza a sobrescribirlos. Los archivos de seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

  Si esta función está deshabilitada, el Agente de red escribe rastreos de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center. No se guardará ningún otro dato de seguimiento.

  No es necesario que habilite la característica de diagnóstico avanzado al momento de crear una tarea. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

  Esta opción está deshabilitada de forma predeterminada.

- **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Los especialistas en soporte técnico de Kaspersky podrían pedirle que cambie el valor predeterminado si, para solucionar un problema, les remite archivos de diagnóstico avanzado con información insuficiente.

11. Haga clic en el botón **Guardar**.

La tarea queda creada y configurada.

Si los resultados de la tarea contienen una advertencia del error 0x80240033 "Error del Agente de Windows Update 80240033 (" No se pudieron descargar los términos de licencia "), puede resolver este problema a través del Registro de Windows .

## Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea automáticamente cuando se ejecuta el asistente de inicio rápido. Si no ejecutó el asistente, puede crear la tarea manualmente.

A continuación, se describen los ajustes que puede configurar para la tarea *Buscar vulnerabilidades y actualizaciones requeridas* (junto con sus ajustes generales) ya sea al momento de crear la tarea o, si la tarea ya existe, a través de sus propiedades:

- **Buscar vulnerabilidades y actualizaciones catalogadas por Microsoft**

  Al buscar vulnerabilidades y actualizaciones, Kaspersky Security Center utiliza la información sobre las actualizaciones de Microsoft aplicables desde la fuente de actualizaciones de Microsoft, las cuales están disponibles en este momento.

  Podría deshabilitar esta opción si, por ejemplo, ha creado tareas diferentes (con configuraciones diferentes) para las actualizaciones de Microsoft y para las actualizaciones de aplicaciones de terceros.

  Esta opción está activada de forma predeterminada.

  La información sobre las actualizaciones opcionales de Microsoft Windows no se envía al Servidor de administración.

- **Conectarse al servidor de actualizaciones para actualizar los datos**

El Agente de Windows Update del dispositivo administrado se conectará al origen de actualizaciones de Microsoft. Los siguientes servidores pueden actuar como orígenes de actualizaciones de Microsoft:

- Servidor de administración de Kaspersky Security Center (consulte la configuración de la directiva del Agente de red)
- Un servidor Windows Server con Microsoft Windows Server Update Services (WSUS) que se encuentre instalado en la red de su organización
- Los servidores de actualizaciones de Microsoft

Cuando esta opción está habilitada, el Agente de Windows Update del dispositivo administrado se conecta al origen de actualizaciones de Microsoft para obtener información actualizada sobre las actualizaciones de Microsoft Windows aplicables.

Cuando esta opción está deshabilitada, el Agente de actualización de Windows del dispositivo administrado usa la información sobre las actualizaciones de Microsoft Windows aplicables que el origen de actualizaciones brindó en un momento anterior.

Conectarse al origen de actualizaciones de Microsoft puede consumir muchos recursos. Podría deshabilitar esta opción si ha configurado un esquema de conexión periódica a este origen en otra tarea o en la sección **Actualizaciones y vulnerabilidades de software** de las propiedades de la directiva del Agente de red. Si no quiere deshabilitar esta opción, para intentar que el Servidor de administración no se sobrecargue, modifique la programación de la tarea para que se la inicie en un punto aleatorio de un intervalo de 360 minutos.

Esta opción está activada de forma predeterminada.

El modo de obtener las actualizaciones deriva de combinar las siguientes opciones de configuración de la directiva del Agente de red:

- El Agente de Windows Update en un dispositivo administrado se conecta al Servidor de actualizaciones para obtener actualizaciones solo si la opción **Conectarse al servidor de actualizaciones para actualizar los datos** está activada en las propiedades de la tarea *Buscar vulnerabilidades y actualizaciones requeridas* y la opción de **Modo de búsqueda de Windows Update** está configurada como **Activo** en la configuración de la directiva del Agente de red.
- Si no necesita el Agente de red para iniciar una conexión al origen de actualizaciones de Microsoft Windows ni para descargar actualizaciones al realizar la tarea *Análisis de vulnerabilidades*, puede seleccionar la opción **Pasivo** en **Modo de búsqueda de Windows Update**, pero la opción **Conectarse al servidor de actualizaciones para actualizar los datos** debe permanecer habilitada. Así podrá ahorrar recursos y usar las actualizaciones de Windows antes recibidas para analizar las vulnerabilidades. Puede usar el modo pasivo si configura la recepción de actualizaciones de Microsoft Windows de otra manera. Si la recepción de actualizaciones de Microsoft Windows no está configurada de otra manera, no seleccione la opción **Pasivo** en **Modo de búsqueda de Windows Update** porque, en este caso, nunca recibirá información sobre las actualizaciones.
- Independientemente del estado de la opción **Conectarse al servidor de actualizaciones para actualizar los datos** (habilitado o deshabilitado), si se selecciona la opción **Modo de búsqueda de Windows Update** en **Deshabilitado**, Kaspersky Security Center no solicita ninguna información sobre actualizaciones.

- **Buscar vulnerabilidades y actualizaciones catalogadas por Kaspersky para software de terceros**

  Si esta opción está habilitada, Kaspersky Security Center busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft) en el Registro de Windows y en las carpetas especificadas en **Especifique las rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**. Kaspersky determina el alcance de la lista de aplicaciones de terceros compatibles.

  Si esta opción está deshabilitada, Kaspersky Security Center no busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros. Puede que quiera deshabilitar esta opción si utiliza tareas diferentes, con configuraciones diferentes, para las actualizaciones de Microsoft Windows y para las actualizaciones de aplicaciones de terceros.

  Esta opción está activada de forma predeterminada.

- **Especifique las rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**

  Carpetas en las que Kaspersky Security Center buscará aplicaciones de terceros que requieran la instalación de actualizaciones o que tengan vulnerabilidades que deban repararse. Puede utilizar variables del sistema.

  Especifique las carpetas en las que se instalan las aplicaciones. De forma predeterminada, la lista contiene carpetas del sistema en las que se instalan la mayoría de las aplicaciones.

- **Habilitar diagnóstico avanzado**

  Si esta función está habilitada, el Agente de red escribe archivos de seguimiento, incluso si la escritura de archivos de seguimiento está deshabilitada para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center. Los datos de seguimiento se guardan en dos archivos sucesivamente; el tamaño total de ambos archivos está determinado por el valor de la opción **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando los archivos alcanzan su límite de tamaño, el Agente de red comienza a sobrescribirlos. Los archivos de seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

  Si esta función está deshabilitada, el Agente de red escribe rastreos de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center. No se guardará ningún otro dato de seguimiento.

  No es necesario que habilite la característica de diagnóstico avanzado al momento de crear una tarea. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

  Esta opción está deshabilitada de forma predeterminada.

- **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Los especialistas en soporte técnico de Kaspersky podrían pedirle que cambie el valor predeterminado si, para solucionar un problema, les remite archivos de diagnóstico avanzado con información insuficiente.

## Recomendaciones para programar la tarea

Al programar la tarea *Buscar vulnerabilidades y actualizaciones requeridas*, asegúrese de que las opciones **Ejecutar tareas no realizadas** y **Utilizar retardo aleatorio automático para el inicio de la tarea** estén habilitadas.

De manera predeterminada, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* está configurada para iniciarse de forma manual. Si, debido a las reglas de la organización, los dispositivos se encontraran apagados en el momento en que debiera ejecutarse la tarea, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* se ejecutará una vez que los dispositivos se vuelvan a encender, es decir, en la mañana del día siguiente. Esto puede ser inconveniente porque los análisis de vulnerabilidades pueden hacer que aumente la carga en los subsistemas de disco y CPU. Debe buscar que la programación de la tarea se adecue a las reglas dispuestas por su organización.

## Crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades

Para utilizar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, debe tener una licencia de Administración de vulnerabilidades y parches.

Utilice la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para aplicar actualizaciones y reparar vulnerabilidades en las aplicaciones de terceros (incluidas las de Microsoft) instaladas en los dispositivos administrados. La tarea permite instalar múltiples actualizaciones y reparar múltiples vulnerabilidades siguiendo un conjunto de reglas.

Si desea usar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para instalar actualizaciones o reparar vulnerabilidades, realice alguna de las siguientes acciones:

- Ejecute el Asistente de instalación de actualizaciones o el Asistente de reparación de vulnerabilidades.
- Cree una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.
- Agregue una regla de instalación de actualizaciones a una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* existente.

*Para crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.
3. Para la aplicación de Kaspersky Security Center, seleccione el tipo de tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades**.

   Si la tarea no aparece, compruebe si su cuenta tiene los derechos de **Lectura**, **Modificación**, y **Ejecución** para el área funcional **Administración del sistema**: **Administración de vulnerabilidades y parches** área funcional. Sin estos derechos de acceso, no puede crear y configurar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.
4. Escriba un nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).
5. Seleccione los dispositivos a los que se asignará la tarea.

6. Defina las reglas de instalación de actualizaciones y luego configure los siguientes ajustes:

- **Comenzar la instalación cuando se esté por reiniciar o apagar el dispositivo**

  Si esta opción está habilitada, las actualizaciones se instalarán en el momento en el que los dispositivos se reinicien o se apaguen. De lo contrario, las actualizaciones se instalarán siguiendo la programación que se defina.

  Utilice esta opción si la instalación de las actualizaciones podría afectar el rendimiento de los dispositivos.

  Esta opción está deshabilitada de forma predeterminada.

- **Instalar los componentes generales obligatorios del sistema**

  Si esta opción está habilitada, antes de que se instale una actualización, la aplicación instalará automáticamente todos los componentes generales del sistema que la actualización requiera para instalarse (los llamados "requisitos previos"). Una actualización podría requerir, por ejemplo, que esté instalada cierta actualización del sistema operativo.

  Si esta opción está deshabilitada, posiblemente tenga que instalar los requisitos previos manualmente.

  Esta opción está deshabilitada de forma predeterminada.

- **Permitir que se instalen versiones nuevas de las aplicaciones durante la actualización**

  Si esta opción está habilitada, las actualizaciones podrán cambiar la versión del software actualizado por una más reciente.

  Si esta opción está deshabilitada, los cambios de versión no estarán permitidos. Para instalar una versión más reciente de una aplicación, deberá usar una tarea diferente o proceder en forma manual. Podría usar esta opción si, por ejemplo, desea evaluar el cambio de versión en una infraestructura de prueba o si sabe que la versión más reciente no es compatible con la infraestructura de su empresa.

  Esta opción está activada de forma predeterminada.

  > Los cambios de versión pueden ocasionar problemas de funcionamiento en las aplicaciones dependientes instaladas en los dispositivos cliente.

- **Descargar las actualizaciones en el dispositivo sin instalarlas**

  Si esta opción está habilitada, la aplicación descargará las actualizaciones disponibles en los dispositivos, pero no las instalará automáticamente. Podrá instalar las actualizaciones descargadas manualmente.

  Las actualizaciones de Microsoft se descargan en el sistema de almacenamiento de Windows. Las actualizaciones para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky ni Microsoft) se descargan en la carpeta especificada en el campo **Descargar actualizaciones en**.

  Si esta opción está deshabilitada, las actualizaciones se instalarán en los dispositivos automáticamente.

  Esta opción está deshabilitada de forma predeterminada.

- **Descargar actualizaciones en**

Esta carpeta se utiliza para descargar las actualizaciones para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky ni Microsoft).

- **Habilitar diagnóstico avanzado**

  Si esta función está habilitada, el Agente de red escribe archivos de seguimiento, incluso si la escritura de archivos de seguimiento está deshabilitada para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center. Los datos de seguimiento se guardan en dos archivos sucesivamente; el tamaño total de ambos archivos está determinado por el valor de la opción **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando los archivos alcanzan su límite de tamaño, el Agente de red comienza a sobrescribirlos. Los archivos de seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

  Si esta función está deshabilitada, el Agente de red escribe rastreos de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center. No se guardará ningún otro dato de seguimiento.

  No es necesario que habilite la característica de diagnóstico avanzado al momento de crear una tarea. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

  Esta opción está deshabilitada de forma predeterminada.

- **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Los especialistas en soporte técnico de Kaspersky podrían pedirle que cambie el valor predeterminado si, para solucionar un problema, les remite archivos de diagnóstico avanzado con información insuficiente.

7. Defina las opciones de reinicio del sistema operativo:

- **No reiniciar el dispositivo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

- **Reiniciar el dispositivo**

  Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

  Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**

  Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

  Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

  Si no habilita esta opción, la solicitud se mostrará una sola vez.

- **Reiniciar después de (min)**

  Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

  Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Tiempo de espera antes del cierre forzado de aplicaciones en sesiones bloqueadas (min)**

Las aplicaciones se cerrarán por la fuerza cuando el dispositivo del usuario se bloquee (sea manualmente o en forma automática tras un tiempo de inactividad).

Si esta opción está habilitada, las aplicaciones del dispositivo bloqueado se cerrarán por la fuerza luego de transcurra el intervalo especificado en el campo de entrada.

Si esta opción está deshabilitada, las aplicaciones del dispositivo bloqueado no se cerrarán.

Esta opción está deshabilitada de forma predeterminada.

8. Si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.

9. Haga clic en el botón **Finalizar**.

   Se crea la tarea y se la agrega a la lista de tareas.

10. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.

11. En la ventana de propiedades de la tarea, modifique los ajustes generales de la tarea según resulte necesario.

12. Haga clic en el botón **Guardar**.

    La tarea queda creada y configurada.

Si los resultados de la tarea contienen una advertencia del error 0x80240033 "Error del Agente de actualización de Windows 80240033 (" No se pudieron descargar los términos del periodo de vigencia de la licencia "), puede resolver este problema a través del Registro de Windows .

## Agregar reglas de instalación de actualizaciones

Esta función solo está disponible con una licencia de Administración de vulnerabilidades y parches.

Si desea utilizar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para instalar actualizaciones de software o reparar vulnerabilidades en sus aplicaciones, debe definir reglas de instalación de actualizaciones. Estas reglas determinan qué actualizaciones se deben instalar y qué vulnerabilidades se deben reparar.

La configuración exacta depende de si la regla se crea para todas las actualizaciones, para actualizaciones de Windows Update o para actualizaciones publicadas para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky y Microsoft). Cuando agregue una regla para actualizaciones de Windows Update o para actualizaciones de aplicaciones de terceros, podrá seleccionar las aplicaciones específicas (y las versiones puntuales de esas aplicaciones) para las que quiera instalar actualizaciones. Cuando agregue una regla para todas las actualizaciones, podrá seleccionar las actualizaciones específicas que quiera instalar y las vulnerabilidades puntuales que quiera reparar mediante la instalación de actualizaciones.

Para agregar una regla de instalación de actualizaciones, puede optar por cualquiera de estos métodos:

- Agregue la regla cuando esté creando una nueva tarea Instalar actualizaciones requeridas y reparar vulnerabilidades.
- Agregue la regla en la pestaña **Configuración de la aplicación** de la ventana de propiedades de una tarea de *Instalar actualizaciones requeridas y reparar vulnerabilidades*.
- Utilice el Asistente de instalación de actualizaciones o el Asistente de reparación de vulnerabilidades.

*Para agregar una nueva regla para todas las actualizaciones, haga lo siguiente:*

1. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Siguiente**.

2. En la página **Tipo de regla**, seleccione **Regla para todas las actualizaciones**.

3. En la página **Criterios generales**, use las listas desplegables para definir los siguientes ajustes:

   - **Conjunto de actualizaciones para instalar**

     Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

     - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

   - **Reparar vulnerabilidades que tengan o superen este nivel de gravedad**

     Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

     Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

     Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

     Esta opción está deshabilitada de forma predeterminada.

4. En la página **Actualizaciones**, seleccione las actualizaciones que se instalarán:

   - **Instalar todas las actualizaciones adecuadas**

     Se instalarán todas las actualizaciones de software que cumplan con los criterios especificados en la página **Criterios generales** del asistente. Esta es la opción seleccionada por defecto.

   - **Instalar solo las actualizaciones de la lista**

     Se instalarán únicamente las actualizaciones de software que seleccione manualmente en la lista. La lista contiene todas las actualizaciones de software disponibles.

     Existen situaciones en las que querrá elegir manualmente las actualizaciones que se instalarán: podría suceder, por ejemplo, que quiera evaluar ciertas actualizaciones en un entorno de prueba, que quiera actualizar solo las aplicaciones que considere importantes o que necesite actualizar solo algunas aplicaciones puntuales.

     - **Instalar automáticamente todas las actualizaciones de aplicaciones previas requeridas para instalar las actualizaciones seleccionadas**

       Mantenga habilitada esta opción si está de acuerdo en que, para instalar las actualizaciones seleccionadas, se instalen versiones intermedias de las aplicaciones.

       Si deshabilita esta opción, se instalarán únicamente las versiones de las aplicaciones que haya seleccionado. Deshabilite esta opción si quiere que las aplicaciones se actualicen en forma directa, sin que se trate de instalar versiones intermedias. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

       A modo de ejemplo, imagine que un dispositivo tiene instalada la versión 3 de una aplicación. Quiere actualizar esa versión a la 5, pero la versión 5 solo se puede instalar sobre la versión 4. Si esta opción está habilitada, el software instalará primero la versión 4 y luego la versión 5. Si esta opción está deshabilitada, el software no podrá actualizar la aplicación.

       Esta opción está activada de forma predeterminada.

5. En la página **Vulnerabilidades**, seleccione las vulnerabilidades que se repararán al instalar las actualizaciones seleccionadas:

   - **Reparar todas las vulnerabilidades que coincidan con otros criterios**

     Se repararán todas las vulnerabilidades que cumplan con los criterios especificados en la página **Criterios generales** del asistente. Esta es la opción seleccionada por defecto.

   - **Reparar solo las vulnerabilidades de la lista**

     Se repararán únicamente las vulnerabilidades que seleccione manualmente en la lista. La lista contiene todas las vulnerabilidades detectadas.

     Existen situaciones en las que querrá elegir manualmente las vulnerabilidades que se repararán: podría suceder, por ejemplo, que quiera verificar en un entorno de prueba que las vulnerabilidades se puedan reparar, que quiera reparar las vulnerabilidades solo en las aplicaciones que considere importantes o que prefiera reparar las vulnerabilidades solo en ciertas aplicaciones puntuales.

6. En la página **Nombre**, escriba un nombre para la regla que está agregando. Podrá cambiar este nombre más tarde, en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Cuando el Asistente de creación de reglas llegue a su fin, se agregará la nueva regla. La encontrará en la lista de reglas del Asistente para crear nueva tarea o en las propiedades de la tarea.

*Para agregar una nueva regla para actualizaciones de Windows Update, haga lo siguiente:*

1. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Siguiente**.

2. En la página **Tipo de regla**, seleccione **Regla para Windows Update**.

3. En la página **Criterios generales**, defina los siguientes ajustes:

- Conjunto de actualizaciones para instalar

  Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

  - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
  - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
  - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

- Reparar vulnerabilidades que tengan o superen este nivel de gravedad

  Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

  Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

  Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

  Esta opción está deshabilitada de forma predeterminada.

- Reparar vulnerabilidades con un nivel de gravedad de MSRC igual o mayor que

  Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

  Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que el Centro de respuestas de seguridad de Microsoft (MSRC) haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

  Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

  Esta opción está deshabilitada de forma predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desee instalar actualizaciones. Por defecto, están seleccionadas todas las aplicaciones.

5. En la página **Categorías de actualizaciones**, seleccione las categorías de actualizaciones que se instalarán. Las categorías son las mismas que se usan en el Catálogo de Microsoft Update. Por defecto, están seleccionadas todas las categorías.

6. En la página **Nombre**, escriba un nombre para la regla que está agregando. Podrá cambiar este nombre más tarde, en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Cuando el Asistente de creación de reglas llegue a su fin, se agregará la nueva regla. La encontrará en la lista de reglas del Asistente para crear nueva tarea o en las propiedades de la tarea.

*Para agregar una nueva regla para actualizaciones de aplicaciones de terceros, haga lo siguiente:*

1. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Siguiente**.

2. En la página **Tipo de regla**, seleccione **Regla para las actualizaciones de terceros**.

3. En la página **Criterios generales**, defina los siguientes ajustes:

   - Conjunto de actualizaciones para instalar

     Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

     - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

   - Reparar vulnerabilidades que tengan o superen este nivel de gravedad

     Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

     Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

     Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

     Esta opción está deshabilitada de forma predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desee instalar actualizaciones. Por defecto, están seleccionadas todas las aplicaciones.

5. En la página **Nombre**, escriba un nombre para la regla que está agregando. Podrá cambiar este nombre más tarde, en la sección Configuración de la ventana de propiedades de la tarea creada.

Cuando el Asistente de creación de reglas llegue a su fin, se agregará la nueva regla. La encontrará en la lista de reglas del Asistente para crear nueva tarea o en las propiedades de la tarea.

# Crear la tarea Instalar actualizaciones de Windows Update

La tarea *Instalar actualizaciones de Windows Update* le permite instalar las actualizaciones de software que proporciona el servicio de Windows Update en los dispositivos administrados.

Si no tiene la licencia de la Administración de vulnerabilidades y parches, no puede crear nuevas tareas del tipo *Instalar actualizaciones de Windows Update*. Para instalar nuevas actualizaciones, puede agregarlas a una tarea *Instalar actualizaciones de Windows Update* existente. Recomendamos que utilice la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* en lugar de la tarea *Instalar actualizaciones de Windows Update*. La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* le permitirá instalar múltiples actualizaciones y reparar múltiples vulnerabilidades simultánea y automáticamente utilizando un conjunto de reglas. Además, esta tarea le permite instalar actualizaciones de proveedores de software distintos de Microsoft.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedirle al usuario que la cierre.

*Para crear la tarea "Instalar actualizaciones de Windows Update":*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
3. Para la aplicación de Kaspersky Security Center, seleccione el tipo de tarea **Instalar actualizaciones de Windows Update**.
4. Escriba un nombre para la tarea que está creando.

   El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).
5. Seleccione los dispositivos a los que se asignará la tarea.
6. Haga clic en el botón **Agregar**.

   Se abre la lista de actualizaciones.
7. Seleccione las actualizaciones de Windows Update que desee instalar y, a continuación, haga clic en **Aceptar**.

8. Defina las opciones de reinicio del sistema operativo:

- **No reiniciar el dispositivo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

- **Reiniciar el dispositivo**

  Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

  Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**

  Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

  Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

  Si no habilita esta opción, la solicitud se mostrará una sola vez.

- **Reiniciar después de (min)**

  Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

  Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de aplicaciones en sesiones bloqueadas**

Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

Esta opción está deshabilitada de forma predeterminada.

9. Configure los ajustes relativos a la cuenta:

- **Cuenta predeterminada**

  La tarea se ejecutará utilizando la misma cuenta que la aplicación que realizará la tarea.

  Esta opción está seleccionada de forma predeterminada.

- **Especificar cuenta**

  Complete los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta con la que se ejecutará la tarea. La cuenta debe tener los derechos necesarios para realizar la tarea.

- **Cuenta**

  Cuenta con la que se ejecutará la tarea.

- **Contraseña**

  Contraseña de la cuenta con la que se ejecutará la tarea.

10. Si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.

11. Haga clic en el botón **Finalizar**.

    Se crea la tarea y se la agrega a la lista de tareas.

12. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.

13. En la ventana de propiedades de la tarea, modifique los ajustes generales de la tarea según resulte necesario.

14. Haga clic en el botón **Guardar**.

La tarea queda creada y configurada.

# Ver información sobre las actualizaciones disponibles para el software de terceros

Puede ver la lista de actualizaciones disponibles para las aplicaciones de terceros instaladas en los dispositivos cliente (incluidas las aplicaciones de Microsoft).

*Para ver una lista de las actualizaciones disponibles para las aplicaciones de terceros instaladas en los dispositivos cliente,*

En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Actualizaciones de software**.

Se mostrará una lista con las actualizaciones disponibles.

Puede aplicar un filtro para ver la lista de actualizaciones de software. Para definir el filtro, haga clic en el ícono **Filtrar** (  ) ubicado en la esquina superior derecha de la lista de actualizaciones de software. También puede elegir un filtro preestablecido de la lista desplegable **Filtros preestablecidos**, que se encuentra sobre la lista de vulnerabilidades de software.

*Para ver las propiedades de una actualización:*

1. Haga clic en el nombre de la actualización de software que sea de su interés.
2. Se abre la ventana de propiedades de la actualización, que consta de las siguientes pestañas con información:

- **General**

  Esta pestaña contiene los detalles generales de la actualización seleccionada:

  - Estado de aprobación de la actualización (si desea cambiar este estado, puede elegir uno diferente en la lista desplegable)
  - Categoría de Windows Server Update Services (WSUS) a la que pertenece la actualización
  - Fecha y hora en que se registró la actualización
  - Fecha y hora en que se creó la actualización
  - Nivel de importancia de la actualización
  - Requisitos de instalación impuestos por la actualización
  - Familia de aplicaciones a la que pertenece la actualización
  - Aplicación a la que corresponde la actualización
  - Número de revisión de la actualización

- **Atributos**

Esta pestaña muestra una serie de atributos que permiten buscar más información sobre la actualización seleccionada. Los atributos disponibles dependen de si la actualización fue publicada por Microsoft o por otro desarrollador.

Cuando una actualización proviene de Microsoft, la información disponible en la pestaña es la siguiente:

- Nivel de importancia asignado a la actualización por el Centro de respuestas de seguridad de Microsoft (MSRC)
- Vínculo al artículo de Microsoft Knowledge Base en el que se describe la actualización
- Vínculo al artículo del boletín de seguridad de Microsoft en el que se describe la actualización
- Identificador (id.) de la actualización

Cuando una actualización proviene de otro desarrollador, la información disponible en la pestaña es la siguiente:

- Indicador de si la actualización es un parche o un paquete de distribución completo
- Idioma de localización de la actualización
- Indicador de si la actualización se instaló de forma manual o automática
- Indicador de si la actualización se revocó tras ser instalada
- Vínculo de descarga de la actualización

- **Dispositivos**

  Esta pestaña contiene la lista de dispositivos en los que se encuentra instalada la actualización elegida.

- **Vulnerabilidades reparadas**

  Esta pestaña contiene la lista de vulnerabilidades que pueden repararse con la actualización seleccionada.

- **Cruce de actualizaciones**

  Esta pestaña muestra cualquier "cruce" que pueda existir entre las actualizaciones publicadas para una misma aplicación; en otras palabras, aquí se indica si la actualización seleccionada puede reemplazar a otras actualizaciones o si, por el contrario, puede ser reemplazada por otras. Esta información solo está disponible para actualizaciones de Microsoft.

- **Tareas para instalar esta actualización**

  Esta pestaña contiene una lista de tareas que, por su alcance, pueden usarse para instalar la actualización seleccionada. Desde aquí también se puede crear una nueva tarea de instalación remota para la actualización.

*Para ver las estadísticas de instalación de una actualización:*

1. Marque la casilla ubicada junto a la actualización de software que sea de su interés.
2. Haga clic en el botón **Estadísticas de los estados de instalación de la actualización**.

Se muestra un diagrama con los estados de instalación de la actualización. Si hace clic en un estado, se abrirá una lista con los dispositivos en los que la actualización tenga el estado seleccionado.

Puede ver información sobre las actualizaciones de software disponibles para el software de terceros (incluido el software de Microsoft) instalado en un dispositivo con Windows en particular.

*Para ver una lista de las actualizaciones disponibles para el software de terceros instalado en un dispositivo administrado específico:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.

   Se muestra la lista de dispositivos administrados.
2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo sobre el que quiera información.

   Se muestra la ventana de propiedades del dispositivo seleccionado.
3. En la ventana de propiedades del dispositivo seleccionado, elija la pestaña **Avanzado**.
4. En el panel de la izquierda, elija la sección **Actualizaciones disponibles**. Si solo desea ver las actualizaciones instaladas, seleccione la opción **Mostrar actualizaciones instaladas**.

Se muestra la lista de actualizaciones de software de terceros disponibles para el dispositivo seleccionado.

## Exportar la lista de actualizaciones de software disponibles a un archivo

Puede exportar a un archivo CSV o TXT la lista de actualizaciones disponibles para las aplicaciones de terceros (incluidas las de Microsoft) que se muestra en un momento dado. Una vez que tenga el archivo, podrá almacenarlo para fines estadísticos, enviarlo a la persona que esté a cargo de la seguridad de la información o utilizarlo para otros fines.

*Para exportar a un archivo de texto la lista de actualizaciones disponibles para el software de terceros instalado en todos los dispositivos administrados:*

1. En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Actualizaciones de software**.

   La página muestra una lista de actualizaciones disponibles para el software de terceros instalado en todos los dispositivos administrados.
2. Haga clic en el botón **Exportar a TXT** o en el botón **Exportar a CSV**, dependiendo del formato de exportación que prefiera.

El archivo con la lista de actualizaciones disponibles para el software de terceros, incluido el software de Microsoft, se guardará en el dispositivo que esté utilizando.

*Para exportar a un archivo de texto la lista de actualizaciones disponibles para el software de terceros instalado en un dispositivo administrado específico:*

1. Abra la lista de actualizaciones de software de terceros disponibles para el dispositivo administrado pertinente.
2. Seleccione las actualizaciones de software que desee exportar.

   Omita este paso si desea exportar toda la lista de actualizaciones de software.

   Si desea exportar la lista completa de actualizaciones de software, tenga en cuenta que solo se exportarán las actualizaciones que aparezcan en la página que esté viendo.

   Si desea exportar solo las actualizaciones instaladas, marque la casilla **Mostrar actualizaciones instaladas**.
3. Haga clic en el botón **Exportar a TXT** o en el botón **Exportar a CSV**, dependiendo del formato de exportación que prefiera.

En el dispositivo que esté utilizando, se guardará un archivo con la lista de actualizaciones disponibles para el software de terceros (incluido el software de Microsoft) instalado en el dispositivo administrado seleccionado.

## Aprobar y rechazar actualizaciones de software de terceros

Al configurar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede crear una regla que exija que las actualizaciones que se deban instalar tengan un estado específico. Una regla de actualización puede permitir, por ejemplo, la instalación de estas actualizaciones:

- Solo las actualizaciones aprobadas
- Solo las actualizaciones aprobadas o sin estado definido
- Todas las actualizaciones, independientemente de su estado

Puede aprobar las actualizaciones que deban instalarse y rechazar las que no deban instalarse.

Puede usar el estado *Aprobada* para administrar la instalación de un número modesto de actualizaciones. Cuando necesite instalar muchas actualizaciones, utilice en cambio las reglas que puede configurar en la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Asigne el estado *Aprobada* únicamente a las actualizaciones que no cumplan con los criterios indicados en las reglas. Aprobar un gran número de actualizaciones en forma manual afecta el rendimiento del Servidor de administración y puede, incluso, hacer que se sobrecargue.

*Para aprobar o rechazar una o más actualizaciones:*

1. En el menú principal, vaya a **Operaciones → Administración de parches → Actualizaciones de software**.

   Se mostrará una lista con las actualizaciones disponibles.
2. Seleccione las actualizaciones que desee aprobar o rechazar.
3. Haga clic en **Aprobar** para aprobar las actualizaciones seleccionadas o en **Rechazar** para rechazarlas.

   El valor predeterminado es *Sin definir*.

Los estados de las actualizaciones seleccionadas cambian a los que ha elegido.

Como alternativa, puede cambiar el estado de aprobación en las propiedades de una actualización específica.

*Para aprobar o rechazar una actualización desde sus propiedades:*

1. En el menú principal, vaya a **Operaciones → Administración de parches → Actualizaciones de software**.

   Se mostrará una lista con las actualizaciones disponibles.

2. Haga clic en el nombre de la actualización que desee aprobar o rechazar.

   Se abre la ventana de propiedades de la actualización.

3. En la sección **General**, cambie la opción **Estado de aprobación de la actualización** para elegir el estado de la actualización. Puede seleccionar los estados *Aprobada*, *Rechazada* o *Sin definir*.

4. Haga clic en el botón **Guardar** para guardar los cambios.

El estado de la actualización seleccionada cambia al que ha elegido.

Si asigna el estado **Rechazada** a las actualizaciones de software de un tercero, estas no se instalarán en los dispositivos a los que estén asignadas, pero que aún no las hayan recibido. Las actualizaciones no se eliminarán de los dispositivos en los que ya se encuentren instaladas. Si necesita eliminar estas actualizaciones, hágalo manualmente en forma local.

## Creación de la tarea Realizar la sincronización con Windows Update

Para utilizar la tarea *Sincronización con Windows Update*, deberá tener una licencia de Administración de vulnerabilidades y parches.

Se necesita la tarea *Sincronización con Windows Update* si desea utilizar el Servidor de administración como servidor WSUS. En este caso, el Servidor de administración descarga las actualizaciones de Windows a la base de datos y reparte las actualizaciones de Windows Update a los dispositivos cliente de modo centralizado a través de Agentes de red. Si la red no emplea ningún servidor de WSUS, cada dispositivo cliente descarga por su propia cuenta las actualizaciones de Microsoft desde servidores externos.

La tarea *Sincronización con Windows Update* solo descarga metadatos de los servidores de Microsoft. Kaspersky Security Center descarga las actualizaciones cuando ejecuta una tarea de instalación de actualizaciones y solo las actualizaciones que usted seleccione instalar.

Al ejecutar la tarea **Sincronización con Windows Update**, la aplicación recibe una lista de actualizaciones vigentes de un servidor de actualizaciones de Microsoft. Luego, Kaspersky Security Center compila una lista de actualizaciones que se han desactualizado. Al siguiente inicio de la tarea **Buscar vulnerabilidades y actualizaciones requeridas**, Kaspersky Security Center marca todas las actualizaciones desactualizadas y configura su momento de eliminación. Al siguiente inicio de la tarea **Sincronización con Windows Update**, se eliminan todas las actualizaciones marcadas para su eliminación hace 30 días. Kaspersky Security Center también comprueba las actualizaciones desactualizadas que se marcaron para su eliminación hace más de 180 días y, luego, elimina estas actualizaciones más antiguas.

Cuando se completa la tarea **Sincronización con Windows Update** y se eliminan las actualizaciones desactualizadas, es posible que la base de datos aún tenga los códigos hash pertenecientes a los archivos de las actualizaciones eliminadas, así como los archivos correspondientes en los archivos de %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles (si se descargaron anteriormente). Puede ejecutar la tarea **Mantenimiento del Servidor de administración** para eliminar estos registros desactualizados de la base de datos y de los archivos correspondientes.

*Para crear la tarea Sincronización con Windows Update:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.
3. Para la aplicación de Kaspersky Security Center, seleccione el tipo de tarea l **Sincronización con Windows Update**.
4. Escriba un nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).
5. Habilite la opción **Descargar archivos de instalación rápida** si desea que los archivos de actualización rápida se descarguen al ejecutar la tarea.

   Cuando Kaspersky Security Center realiza la sincronización de actualizaciones con los servidores de Windows Update, guarda información sobre todos los distintos archivos en la base de datos del Servidor de administración. Todos los archivos requeridos para una actualización también se descargan a la unidad durante la interacción con el Agente de Windows Update. En particular, Kaspersky Security Center guarda la información sobre archivos de actualización expresos en la base de datos y los descarga cuando sea necesario. Descargar archivos de actualización rápida genera una reducción del espacio libre en la unidad.

   Para evitar una disminución en el volumen del espacio de disco y reducir el tráfico, desactive la opción **Descargar archivos de instalación rápida**.
6. Seleccione las aplicaciones para las que desea descargar actualizaciones.

   Si la casilla **Todas las aplicaciones** se selecciona, las actualizaciones se descargarán para todas las aplicaciones existentes, y para todas las aplicaciones que se puedan publicar en el futuro.
7. Seleccione las categorías de actualizaciones que desea descargar al Servidor de administración.

   Si la casilla **Todas las categorías** se selecciona, las actualizaciones se descargarán para todas las categorías de actualizaciones existentes, y para todas las categorías que se puedan publicar en el futuro.
8. Seleccione los idiomas de localización de las actualizaciones que desea descargar al Servidor de administración. Seleccione una de las siguientes opciones:

   - **Descargar todos los idiomas, incluidos los nuevos**

     Si se selecciona esta opción, todos los idiomas de localización de las actualizaciones disponibles se descargarán en el Servidor de administración. Esta opción está seleccionada de forma predeterminada.

   - **Descargar los idiomas seleccionados**

     Si se selecciona esta opción, podrá elegir de la lista los idiomas de localización de las actualizaciones que se descargarán en el Servidor de administración.

9. Especifique qué cuenta usar al ejecutar la tarea. Seleccione una de las siguientes opciones:

   - **Cuenta predeterminada**

     La tarea se ejecutará utilizando la misma cuenta que la aplicación que realizará la tarea.

     Esta opción está seleccionada de forma predeterminada.

   - **Especificar cuenta**

     Complete los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta con la que se ejecutará la tarea. La cuenta debe tener los derechos necesarios para realizar la tarea.

10. Si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.

11. Haga clic en el botón **Finalizar**.

    Se crea la tarea y se la agrega a la lista de tareas.

12. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.

13. En la ventana de propiedades de la tarea, modifique los ajustes generales de la tarea según resulte necesario.

14. Haga clic en el botón **Guardar**.

La tarea queda creada y configurada.

## Actualización automática de aplicaciones de terceros

Algunas aplicaciones de terceros se pueden actualizar automáticamente. Quien determina si una aplicación es compatible con la función de actualización automática es su desarrollador o proveedor. Si una aplicación de terceros instalada en un dispositivo administrado se puede actualizar automáticamente, podrá configurar el ajuste de actualización automática en las propiedades de esa aplicación. Luego de que modifique este ajuste, las instancias del Agente de red implementarán el nuevo valor en cada dispositivo administrado que tenga instalada esa aplicación.

El ajuste de actualización automática es independiente de los demás objetos y ajustes de la característica Administración de vulnerabilidades y parches. Este ajuste, por ejemplo, no se ve afectado por los estados de aprobación de las actualizaciones ni por las distintas tareas de instalación de actualizaciones, como *Instalar actualizaciones requeridas y reparar vulnerabilidades*, *Instalar actualizaciones de Windows Update* y *Reparar vulnerabilidades*.

*Para configurar el ajuste de actualización automática para una aplicación creada por un tercero:*

1. En el menú principal, vaya a **Operaciones → Aplicaciones de terceros → Registro de aplicaciones**.

2. Haga clic en el nombre de la aplicación para la que desee modificar el ajuste de actualización automática.

   Puede usar la columna **Estado de las actualizaciones automáticas** para filtrar la lista y simplificar la búsqueda.

   Se abrirá la ventana de propiedades de la aplicación.

3. En la sección **General**, seleccione un valor para el siguiente ajuste:

   **Estado de las actualizaciones automáticas**

   Seleccione una de las siguientes opciones:

   - **Sin definir**

     Se deshabilitará la función de actualización automática. Kaspersky Security Center instala actualizaciones de aplicaciones de terceros mediante las siguientes tareas: *Instalar actualizaciones requeridas y reparar vulnerabilidades*, *Instalar actualizaciones de Windows Update* y *Reparar vulnerabilidades*.

   - **Permitido**

     Las actualizaciones que el proveedor publique para la aplicación se instalarán automáticamente en los dispositivos administrados. No se requerirá ninguna otra acción.

   - **Bloqueado**

     Las actualizaciones para la aplicación no se instalarán automáticamente. Kaspersky Security Center instala actualizaciones de aplicaciones de terceros mediante las siguientes tareas: *Instalar actualizaciones requeridas y reparar vulnerabilidades*, *Instalar actualizaciones de Windows Update* y *Reparar vulnerabilidades*.

4. Haga clic en el botón **Guardar** para guardar los cambios.

El valor definido para el ajuste de actualización automática se implementa en la aplicación seleccionada.

# Reparación de vulnerabilidades en el software de terceros

En esta sección, se describen las características de Kaspersky Security Center relacionadas con la reparación de vulnerabilidades en el software instalado en dispositivos administrados.

## Procedimiento: búsqueda y reparación de vulnerabilidades de software de terceros

En esta sección, se describe un escenario para buscar y reparar vulnerabilidades en dispositivos administrados que utilizan el sistema operativo Windows. Puede buscar y reparar vulnerabilidades de software en el sistema operativo y en las aplicaciones de terceros, incluidas las de Microsoft.

## Requisitos previos

- Kaspersky Security Center está desplegado en su organización.
- Hay dispositivos administrados que ejecutan Windows en su organización.
- Se requiere conexión a Internet para que el Servidor de administración realice las siguientes tareas:
  - Hacer una lista de reparaciones recomendadas para vulnerabilidades en el software de Microsoft. Los especialistas de Kaspersky crean y actualizan periódicamente esta lista.
  - Reparar vulnerabilidades en software de terceros que no sea el software de Microsoft.

## Etapas

El proceso para buscar y reparar vulnerabilidades de software se divide en etapas:

1. **Análisis en busca de vulnerabilidades en el software instalado en los dispositivos administrados**

   Para encontrar vulnerabilidades en el software instalado en los dispositivos administrados, ejecute la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Cuando se completa esta tarea, Kaspersky Security Center recibe las listas de vulnerabilidades detectadas y las actualizaciones necesarias para el software de terceros instalado en los dispositivos que especificó en las propiedades de la tarea.

   La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea automáticamente con el Asistente de inicio rápido de Kaspersky Security Center. Si no ejecutó el asistente de inicio rápido, hágalo ahora o cree la tarea manualmente.

   Instrucciones:

   - Consola de administración: Análisis de aplicaciones en busca de vulnerabilidades, Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas
   - Kaspersky Security Center Web Console: Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas, Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

2. **Analizar la lista de vulnerabilidades de software detectadas**

   Abra la lista **Vulnerabilidades de software** y decida qué vulnerabilidades desea reparar. Para ver información detallada sobre una vulnerabilidad, haga clic en el nombre de la misma en la lista. La aplicación le da acceso a estadísticas sobre el estado de cada vulnerabilidad en los dispositivos administrados.

   Instrucciones:

   - Consola de administración: visualización de vulnerabilidades de software de información, visualización de estadísticas de vulnerabilidades en dispositivos administrados
   - Kaspersky Security Center Web Console: Consultar información sobre vulnerabilidades de software, Visualización de estadísticas de vulnerabilidades en dispositivos administrados

3. **Configurar la reparación de vulnerabilidades**

   Una vez que se han detectado las vulnerabilidades de software, puede repararlas en los dispositivos administrados con las tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades* y *Reparar vulnerabilidades*.

Utilice la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para aplicar actualizaciones y reparar vulnerabilidades en las aplicaciones de terceros (incluidas las de Microsoft) instaladas en los dispositivos administrados. La tarea permite instalar múltiples actualizaciones y reparar múltiples vulnerabilidades siguiendo un conjunto de reglas. Tenga en cuenta que esta tarea se puede crear únicamente si se cuenta con una licencia para la función Administración de vulnerabilidades y parches. Para corregir vulnerabilidades de software, la a tarea utiliza actualizaciones de software recomendadas *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

La tarea *Reparar vulnerabilidades* no requiere la opción de licencia correspondiente a la función Administración de vulnerabilidades y parches. Para utilizar esta tarea, debe especificar manualmente las correcciones del usuario para las vulnerabilidades en el software de terceros que figuran en la configuración de la tarea. La tarea *Reparar vulnerabilidades* utiliza correcciones recomendadas para el software de Microsoft y correcciones de usuario para software de terceros.

Puede crear estas tareas en forma manual o a través de Asistente de reparación de vulnerabilidades, que las crea en forma automática.

Instrucciones:

- Consola de administración: selección de soluciones de usuario para vulnerabilidades en software de terceros, reparación de la vulnerabilidad en aplicaciones
- Kaspersky Security Center Web Console: Selección de soluciones de usuario para vulnerabilidades en el software de terceros, Reparación de vulnerabilidades en software de terceros, Creación de la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades

**4 Programar las tareas**

Para asegurarse de que la lista de vulnerabilidades siempre esté actualizada, defina una programación que haga que la tarea *Buscar vulnerabilidades y actualizaciones requeridas* se ejecute automáticamente de tanto en tanto. Se recomienda una frecuencia promedio de una vez a la semana.

Si creó la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede programarla para que se ejecute con igual o menor frecuencia que la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Aunque puede definir una programación para la tarea *Reparar vulnerabilidades*, tenga en cuenta que, cada vez que esta se inicie, deberá seleccionar los parches que se aplicarán al software de Microsoft o de otros desarrolladores.

Cuando programe las tareas, asegúrese de que las tareas para reparar vulnerabilidades se inicien después de que finalice la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

**5 Ignorar vulnerabilidades de software (opcional)**

Puede ignorar aquellas vulnerabilidades de software que no desee reparar en ninguno de los dispositivos administrados o en algunos dispositivos administrados específicos.

Instrucciones:

- Consola de administración: ignorar las vulnerabilidades de software
- Kaspersky Security Center Web Console: Ignorar las vulnerabilidades de software

**6 Ejecutar una tarea de reparación de vulnerabilidades**

Inicie las tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades* o *Reparar vulnerabilidad*. Cuando se complete la tarea, asegúrese de que tenga el estado *Completada correctamente* en la lista de tareas.

**7 Crear el informe sobre los resultados de la reparación de vulnerabilidades de software (opcional)**

Para ver estadísticas detalladas sobre la reparación de vulnerabilidades, genere el Informe de vulnerabilidades. El informe le indicará qué vulnerabilidades de software no se corrigieron. Ello le dará un panorama sobre la búsqueda y reparación de vulnerabilidades en el software de terceros (incluido el software de Microsoft) instalado en su organización.

Instrucciones:

- Consola de administración: Crear y ver un informe
- Kaspersky Security Center Web Console: Generar y ver un informe

8. **Revisar la configuración de la búsqueda y reparación de vulnerabilidades en el software de terceros**

   Asegúrese de haber hecho lo siguiente:

   - Obtenido y revisado la lista de vulnerabilidades de software detectadas en los dispositivos administrados.
   - Ignorado las vulnerabilidades de software si así lo deseaba.
   - Configurado la tarea para reparar vulnerabilidades.
   - Programado las tareas de encontrar y reparar vulnerabilidades de software para que comiencen secuencialmente.
   - Comprobado que se haya ejecutado la tarea para reparar vulnerabilidades de software.

### Resultados

Si creó y configuró la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, las vulnerabilidades se repararán en los dispositivos administrados automáticamente. Cuando se ejecuta, la tarea compara la lista de actualizaciones de software disponibles con las reglas especificadas en su configuración. Todas las actualizaciones de software que cumplan con los criterios especificados en las reglas se descargarán en el repositorio del Servidor de administración y se instalarán para reparar las vulnerabilidades de software.

Si creó la tarea *Reparar vulnerabilidades*, solo se corregirán las vulnerabilidades presentes en el software de Microsoft.

## Acerca de la búsqueda y reparación de vulnerabilidades de software

Kaspersky Security Center detecta y corrige vulnerabilidades de software en dispositivos administrados que ejecutan los sistemas operativos de Microsoft Windows. La solución puede detectar vulnerabilidades tanto en el sistema operativo como en aplicaciones desarrolladas por Microsoft y otros terceros.

La función de actualizaciones (incluido el suministro de actualizaciones para las firmas antivirus y la base de código) y la función de KSN pueden dejar de estar disponibles en el software en el territorio de EE. UU.

### Búsqueda de vulnerabilidades de software

Para encontrar vulnerabilidades de software, Kaspersky Security Center utiliza funciones de la base de datos de vulnerabilidades conocidas. Los especialistas de Kaspersky crean esta base de datos. Contiene distintos datos sobre cada vulnerabilidad: su descripción, su fecha de detección, su nivel de gravedad y más. Puede ver los detalles de las vulnerabilidades de software en el sitio web de Kaspersky.

Kaspersky Security Center usa la tarea *Buscar vulnerabilidades y actualizaciones requeridas* para encontrar vulnerabilidades de software.

En ciertos casos, las vulnerabilidades detectadas en un sistema operativo Microsoft Windows se pueden reparar utilizando cualquiera de los siguientes métodos:

- Instalar una actualización para el sistema operativo.
- Actualizar el sistema operativo a una versión más reciente (por ejemplo, de Windows 10 a Windows 11).

En este escenario, Kaspersky Security Center muestra dos entradas para la misma vulnerabilidad.

## Reparación de vulnerabilidades de software

Para reparar vulnerabilidades de software, Kaspersky Security Center utiliza actualizaciones de software que emiten los proveedores de software. Los metadatos de las actualizaciones de software se descargan en el repositorio del Servidor de administración después de que se ejecuten las siguientes tareas:

- *Descargar actualizaciones en el repositorio del Servidor de administración*. Esta tarea tiene como objetivo la descarga de metadatos de actualizaciones para software de Kaspersky y de terceros. Esta tarea se crea automáticamente con el asistente de inicio rápido de Kaspersky Security Center. Puede crear una tarea Descargar actualizaciones en el repositorio del Servidor de administración.
- *Sincronización con Windows Update*. Esta tarea tiene como objetivo la descarga de metadatos de actualizaciones para software de Microsoft.

Las actualizaciones de software con las que se corrigen las vulnerabilidades pueden ser paquetes de distribución completos o parches. Las actualizaciones de software diseñadas para corregir vulnerabilidades de software se denominan *reparaciones*. Las *correcciones recomendadas* son aquellas que los especialistas de Kaspersky sugieren instalar. Las *correcciones de usuario* son aquellas que los usuarios eligen instalar manualmente. Para instalar una corrección de usuario, se debe crear un paquete de instalación que contenga esta reparación.

Si no tiene la licencia de Kaspersky Security Center con la función de Administración de vulnerabilidades y parches para corregir las vulnerabilidades de software, puede usar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Esta tarea repara automáticamente varias vulnerabilidades instalando las reparaciones recomendadas. Si utiliza esta tarea, puede configurar manualmente ciertas reglas para la reparación de múltiples vulnerabilidades.

Si no tiene la licencia de Kaspersky Security Center con la función Administración de vulnerabilidades y parches para corregir las vulnerabilidades de software, puede usar la tarea *Reparar vulnerabilidades*. Mediante esta tarea, puede corregir vulnerabilidades instalando correcciones recomendadas para el software de Microsoft y correcciones de usuario para otro software de terceros.

Por seguridad, cada actualización de software de terceros que se instala con la función Administración de vulnerabilidades y parches se somete a un análisis antimalware automático con las tecnologías de Kaspersky Estas tecnologías revisan automáticamente los archivos utilizando técnicas de análisis antivirus, análisis estático, análisis dinámico, análisis de comportamiento en un entorno de pruebas y aprendizaje automático, entre otras.

Los expertos de Kaspersky no realizan análisis manuales de las actualizaciones de software de terceros que puedan instalarse mediante la función Administración de vulnerabilidades y parches. Tampoco buscan vulnerabilidades (conocidas o desconocidas) o funciones no documentadas en las actualizaciones ni las analizan de modos que no se hayan indicado en el párrafo anterior.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedirle al usuario que la cierre.

Para reparar algunas vulnerabilidades de software, deberá aceptar un contrato de licencia de usuario final (EULA) que lo faculte a instalar el software. Si se le solicita aceptar el EULA, hágalo. Si rechaza el EULA, la vulnerabilidad de software correspondiente no se reparará.

## Reparación de vulnerabilidades en el software de terceros

Una vez que ha obtenido la lista de vulnerabilidades de software, puede reparar las vulnerabilidades de software que estén presentes en los dispositivos Windows administrados. Para reparar vulnerabilidades de software en el sistema operativo y en las aplicaciones creadas por terceros (incluido Microsoft), cree y ejecute la tarea *Reparar vulnerabilidades* o la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación afectada está abierta, por ejemplo, podría tener que pedirle al usuario que la cierre.

Como alternativa, para crear una tarea para reparar vulnerabilidades de software, puede optar por estas vías:

- Abra la lista de vulnerabilidades y seleccione las vulnerabilidades que desee reparar.

  Como resultado, se creará una nueva tarea para reparar las vulnerabilidades de software seleccionadas. Si lo prefiere, puede agregar las vulnerabilidades seleccionadas a una tarea existente.

- Utilice el Asistente de reparación de vulnerabilidades.

  El Asistente de reparación de vulnerabilidades solo está disponible con la licencia de la Administración de vulnerabilidades y parches.

  El asistente simplifica la creación y configuración de una tarea de reparación de la vulnerabilidad y le permite eliminar la creación de tareas redundantes que contienen las mismas actualizaciones para instalar.

## Reparar vulnerabilidades de software a través de la lista de vulnerabilidades

*Para reparar vulnerabilidades de software:*

1. Abra una de las listas de vulnerabilidades:

   - Para abrir la lista de vulnerabilidades general, en el menú principal, vaya a **Operaciones** → **Administración de parches** → **Vulnerabilidades de software**.
   - Para abrir la lista de vulnerabilidades de un dispositivo administrado, en el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados** → <nombre del dispositivo> → **Avanzado** → **Vulnerabilidades de software**.
   - Para abrir la lista de vulnerabilidades de una aplicación específica, en el menú principal vaya a **Operaciones** → **Aplicaciones de terceros** → **Registro de aplicaciones** → <nombre de la aplicación> → **Vulnerabilidades**.

   Se muestra una página con una lista de vulnerabilidades detectadas en las aplicaciones de terceros.

2. Seleccione una o más vulnerabilidades de la lista y haga clic en el botón **Reparar vulnerabilidad**.

   Si no se cuenta con la actualización de software recomendada para reparar alguna de las vulnerabilidades seleccionadas, se mostrará un mensaje informativo.

   Para reparar algunas vulnerabilidades de software, se le solicita al usuario que acepte un contrato de licencia de usuario final (EULA) para instalar el software. Deberá aceptar el EULA. Si rechaza el EULA, no se reparará la vulnerabilidad de software correspondiente.

3. Seleccione una de las siguientes opciones:

   - **Nueva tarea**

     Se inicia el Asistente para crear nueva tarea. Si tiene la licencia de la Administración de vulnerabilidades y parches, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* estará preseleccionada. Si no cuenta con la licencia, el tipo de tarea *Reparar vulnerabilidades* estará preseleccionada. Siga los pasos del asistente para completar la creación de la tarea.

   - **Reparar vulnerabilidad (agregar regla a la tarea especificada)**

     Seleccione la tarea a la que desee agregar las vulnerabilidades seleccionadas. Si tiene la licencia de Administración de vulnerabilidades y parches, seleccione la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Se agregará automáticamente a la tarea elegida una nueva regla para corregir las vulnerabilidades seleccionadas. Si no tiene la licencia, seleccione la tarea *Reparar vulnerabilidades*. Las vulnerabilidades seleccionadas se agregarán a las propiedades de la tarea.

     Se abrirá la ventana de propiedades de la tarea. Haga clic en el botón **Guardar** para guardar los cambios.

   Si optó por crear una tarea, se la creará y se la agregará a la lista de tareas disponible en **Activos (dispositivos)** → **Tareas**. Si optó por agregar las vulnerabilidades a una tarea existente, las vulnerabilidades se guardarán en las propiedades de la tarea que haya elegido.

Para reparar las vulnerabilidades de software de terceros, inicie la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Reparar vulnerabilidades*. Si la tarea que creó es *Reparar vulnerabilidades*, deberá especificar manualmente qué actualizaciones se usarán para reparar las vulnerabilidades enumeradas en la configuración de la tarea.

# Reparar vulnerabilidades de software con el Asistente de reparación de vulnerabilidades

El Asistente de reparación de vulnerabilidades solo está disponible con la licencia de la Administración de vulnerabilidades y parches.

*Para reparar vulnerabilidades de software a través del Asistente de reparación de vulnerabilidades:*

1. En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Vulnerabilidades de software**.

   Se muestra una página con una lista de las vulnerabilidades detectadas en las aplicaciones de terceros instaladas en los dispositivos administrados.

2. Marque la casilla ubicada junto a la vulnerabilidad que desee reparar.

3. Haga clic en el botón **Ejecutar el Asistente de reparación de vulnerabilidades**.

   Se iniciará el Asistente de reparación de vulnerabilidades. En la página **Seleccione una tarea de reparación de vulnerabilidades**, verá una lista con las tareas existentes de los siguientes tipos:

   - *Instalar actualizaciones requeridas y reparar vulnerabilidades*
   - *Instalar actualizaciones de Windows Update*
   - *Reparar vulnerabilidades*

   Los dos últimos tipos de tarea no se pueden modificar para instalar nuevas actualizaciones. Para instalar nuevas actualizaciones, solo puede utilizar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

4. Si desea que el asistente muestre solo las tareas que permitan reparar la vulnerabilidad seleccionada, habilite la opción **Mostrar solo las tareas que permitan reparar esta vulnerabilidad**.

5. Elija lo que desea hacer:

- Para iniciar una tarea, marque la casilla ubicada junto al nombre de la tarea en cuestión y haga clic en el botón **Iniciar**.

- Para agregar una nueva regla a una tarea existente, haga lo siguiente:

  a. Marque la casilla ubicada junto al nombre de la tarea pertinente y haga clic en el botón **Agregar regla**.

  b. En la página que se abrirá, configure la nueva regla:

  - Regla para reparar vulnerabilidades de este nivel de gravedad

    Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

    Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al nivel de gravedad de la actualización seleccionada. Los niveles posibles son **Medio**, **Alto** y **Crítico**. Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

    Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

    Esta opción está deshabilitada de forma predeterminada.

  - **Regla para reparar vulnerabilidades por medio de actualizaciones del mismo tipo que la actualización definida como recomendada para la vulnerabilidad seleccionada** (disponible solo para vulnerabilidades de software de Microsoft)

  - **Regla para reparar vulnerabilidades en las aplicaciones del proveedor seleccionado** (disponible solo para vulnerabilidades de software de terceros)

  - **Regla para reparar una vulnerabilidad en todas las versiones de la aplicación seleccionada** (disponible solo para vulnerabilidades de software de terceros)

  - **Regla para reparar la vulnerabilidad seleccionada**

  - Aprobar actualizaciones que reparen esta vulnerabilidad

    Se aprobará la instalación de la actualización seleccionada. Habilite esta opción si ha aplicado reglas de instalación de actualizaciones que solo permitan instalar actualizaciones aprobadas.

    Esta opción está deshabilitada de forma predeterminada.

  c. Haga clic en el botón **Agregar**.

- Para crear una tarea:

  a. Haga clic en el botón **Nueva tarea**.

  b. En la página que se abrirá, configure la nueva regla:

- Regla para reparar vulnerabilidades de este nivel de gravedad

  Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

  Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al nivel de gravedad de la actualización seleccionada. Los niveles posibles son **Medio**, **Alto** y **Crítico**. Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

  Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

  Esta opción está deshabilitada de forma predeterminada.

- **Regla para reparar vulnerabilidades por medio de actualizaciones del mismo tipo que la actualización definida como recomendada para la vulnerabilidad seleccionada** (disponible solo para vulnerabilidades de software de Microsoft)

- **Regla para reparar vulnerabilidades en las aplicaciones del proveedor seleccionado** (disponible solo para vulnerabilidades de software de terceros)

- **Regla para reparar una vulnerabilidad en todas las versiones de la aplicación seleccionada** (disponible solo para vulnerabilidades de software de terceros)

- **Regla para reparar la vulnerabilidad seleccionada**

- Aprobar actualizaciones que reparen esta vulnerabilidad

  Se aprobará la instalación de la actualización seleccionada. Habilite esta opción si ha aplicado reglas de instalación de actualizaciones que solo permitan instalar actualizaciones aprobadas.

  Esta opción está deshabilitada de forma predeterminada.

c. Haga clic en el botón **Agregar**.

Si eligió iniciar una tarea, puede cerrar el asistente. La tarea se completará en segundo plano. No se requieren más acciones.

Si optó por agregar una regla a una tarea existente, se abrirá la ventana de propiedades de la tarea. Encontrará la nueva regla en las propiedades de la tarea. Si lo desea, vea y modifique la regla u otros ajustes de la tarea. Haga clic en el botón **Guardar** para guardar los cambios.

Si eligió crear una tarea, continúe creándola en el Asistente para crear nueva tarea. La nueva regla que haya agregado en el Asistente de reparación de vulnerabilidades aparecerá en el Asistente para crear nueva tarea. Cuando haya completado el asistente, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se agregará a la lista de tareas.

## Crear la tarea Reparar vulnerabilidades

La tarea *Reparar vulnerabilidades* le permite reparar vulnerabilidades de software en dispositivos administrados que ejecutan Windows. Puede reparar vulnerabilidades de software en software de terceros, incluido el software de Microsoft.

Si no tiene la licencia de Administración de vulnerabilidades y parches, no puede crear nuevas tareas del tipo *Reparar vulnerabilidades*. Para reparar vulnerabilidades nuevas, puede agregarlas a una tarea de *Reparar vulnerabilidades* existente. Le recomendamos que utilice la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* en lugar de la tarea *Reparar vulnerabilidades*. La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* le permitirá instalar múltiples actualizaciones y reparar múltiples vulnerabilidades simultánea y automáticamente utilizando un conjunto de reglas.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedirle al usuario que la cierre.

*Para crear la tarea Reparar vulnerabilidades:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Avance por el asistente utilizando el botón **Siguiente**.
3. Para la aplicación Kaspersky Security Center, seleccione el tipo de tarea **Reparar vulnerabilidades**.
4. Escriba un nombre para la tarea que está creando.

   El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).
5. Seleccione los dispositivos a los que se asignará la tarea.
6. Haga clic en el botón **Agregar**.

   Se abre la lista de vulnerabilidades.
7. Seleccione las vulnerabilidades que desee reparar y, a continuación, haga clic en **Aceptar**.

   Las vulnerabilidades de software de Microsoft suelen tener correcciones recomendadas. No se requieren acciones adicionales. Para vulnerabilidades en el software de otros proveedores, primero tiene que especificar una solución de usuario para cada vulnerabilidad que desea arreglar. Después de eso, podrá agregar esas vulnerabilidades en la tarea *Reparar vulnerabilidades*.

8. Defina las opciones de reinicio del sistema operativo:

- **No reiniciar el dispositivo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

- **Reiniciar el dispositivo**

  Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

  Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**

  Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

  Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

  Si no habilita esta opción, la solicitud se mostrará una sola vez.

- **Reiniciar después de (min)**

  Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

  Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de aplicaciones en sesiones bloqueadas**

Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

Esta opción está deshabilitada de forma predeterminada.

9. Configure los ajustes relativos a la cuenta:

- **Cuenta predeterminada**

  La tarea se ejecutará utilizando la misma cuenta que la aplicación que realizará la tarea.

  Esta opción está seleccionada de forma predeterminada.

- **Especificar cuenta**

  Complete los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta con la que se ejecutará la tarea. La cuenta debe tener los derechos necesarios para realizar la tarea.

- **Cuenta**

  Cuenta con la que se ejecutará la tarea.

- **Contraseña**

  Contraseña de la cuenta con la que se ejecutará la tarea.

10. Si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.

11. Haga clic en el botón **Finalizar**.

    Se crea la tarea y se la agrega a la lista de tareas.

12. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.

13. En la ventana de propiedades de la tarea, modifique los ajustes generales de la tarea según resulte necesario.

14. Haga clic en el botón **Guardar**.

La tarea queda creada y configurada.

# Crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades

Para utilizar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, debe tener una licencia de Administración de vulnerabilidades y parches.

Utilice la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para aplicar actualizaciones y reparar vulnerabilidades en las aplicaciones de terceros (incluidas las de Microsoft) instaladas en los dispositivos administrados. La tarea permite instalar múltiples actualizaciones y reparar múltiples vulnerabilidades siguiendo un conjunto de reglas.

Si desea usar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para instalar actualizaciones o reparar vulnerabilidades, realice alguna de las siguientes acciones:

- Ejecute el Asistente de instalación de actualizaciones o el Asistente de reparación de vulnerabilidades.
- Cree una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.
- Agregue una regla de instalación de actualizaciones a una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* existente.

*Para crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.
3. Para la aplicación de Kaspersky Security Center, seleccione el tipo de tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades**.

   Si la tarea no aparece, compruebe si su cuenta tiene los derechos de **Lectura**, **Modificación**, y **Ejecución** para el área funcional **Administración del sistema**: **Administración de vulnerabilidades y parches** área funcional. Sin estos derechos de acceso, no puede crear y configurar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.
4. Escriba un nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).
5. Seleccione los dispositivos a los que se asignará la tarea.

6. Defina las reglas de instalación de actualizaciones y luego configure los siguientes ajustes:

- **Comenzar la instalación cuando se esté por reiniciar o apagar el dispositivo**

  Si esta opción está habilitada, las actualizaciones se instalarán en el momento en el que los dispositivos se reinicien o se apaguen. De lo contrario, las actualizaciones se instalarán siguiendo la programación que se defina.

  Utilice esta opción si la instalación de las actualizaciones podría afectar el rendimiento de los dispositivos.

  Esta opción está deshabilitada de forma predeterminada.

- **Instalar los componentes generales obligatorios del sistema**

  Si esta opción está habilitada, antes de que se instale una actualización, la aplicación instalará automáticamente todos los componentes generales del sistema que la actualización requiera para instalarse (los llamados "requisitos previos"). Una actualización podría requerir, por ejemplo, que esté instalada cierta actualización del sistema operativo.

  Si esta opción está deshabilitada, posiblemente tenga que instalar los requisitos previos manualmente.

  Esta opción está deshabilitada de forma predeterminada.

- **Permitir que se instalen versiones nuevas de las aplicaciones durante la actualización**

  Si esta opción está habilitada, las actualizaciones podrán cambiar la versión del software actualizado por una más reciente.

  Si esta opción está deshabilitada, los cambios de versión no estarán permitidos. Para instalar una versión más reciente de una aplicación, deberá usar una tarea diferente o proceder en forma manual. Podría usar esta opción si, por ejemplo, desea evaluar el cambio de versión en una infraestructura de prueba o si sabe que la versión más reciente no es compatible con la infraestructura de su empresa.

  Esta opción está activada de forma predeterminada.

  > Los cambios de versión pueden ocasionar problemas de funcionamiento en las aplicaciones dependientes instaladas en los dispositivos cliente.

- **Descargar las actualizaciones en el dispositivo sin instalarlas**

  Si esta opción está habilitada, la aplicación descargará las actualizaciones disponibles en los dispositivos, pero no las instalará automáticamente. Podrá instalar las actualizaciones descargadas manualmente.

  Las actualizaciones de Microsoft se descargan en el sistema de almacenamiento de Windows. Las actualizaciones para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky ni Microsoft) se descargan en la carpeta especificada en el campo **Descargar actualizaciones en**.

  Si esta opción está deshabilitada, las actualizaciones se instalarán en los dispositivos automáticamente.

  Esta opción está deshabilitada de forma predeterminada.

- **Descargar actualizaciones en**

Esta carpeta se utiliza para descargar las actualizaciones para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky ni Microsoft).

- **Habilitar diagnóstico avanzado**

  Si esta función está habilitada, el Agente de red escribe archivos de seguimiento, incluso si la escritura de archivos de seguimiento está deshabilitada para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center. Los datos de seguimiento se guardan en dos archivos sucesivamente; el tamaño total de ambos archivos está determinado por el valor de la opción **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando los archivos alcanzan su límite de tamaño, el Agente de red comienza a sobrescribirlos. Los archivos de seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

  Si esta función está deshabilitada, el Agente de red escribe rastreos de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center. No se guardará ningún otro dato de seguimiento.

  No es necesario que habilite la característica de diagnóstico avanzado al momento de crear una tarea. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

  Esta opción está deshabilitada de forma predeterminada.

- **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Los especialistas en soporte técnico de Kaspersky podrían pedirle que cambie el valor predeterminado si, para solucionar un problema, les remite archivos de diagnóstico avanzado con información insuficiente.

7. Defina las opciones de reinicio del sistema operativo:

- **No reiniciar el dispositivo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

- **Reiniciar el dispositivo**

  Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

  Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**

  Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

  Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

  Si no habilita esta opción, la solicitud se mostrará una sola vez.

- **Reiniciar después de (min)**

  Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

  Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Tiempo de espera antes del cierre forzado de aplicaciones en sesiones bloqueadas (min)**

Las aplicaciones se cerrarán por la fuerza cuando el dispositivo del usuario se bloquee (sea manualmente o en forma automática tras un tiempo de inactividad).

Si esta opción está habilitada, las aplicaciones del dispositivo bloqueado se cerrarán por la fuerza luego de transcurra el intervalo especificado en el campo de entrada.

Si esta opción está deshabilitada, las aplicaciones del dispositivo bloqueado no se cerrarán.

Esta opción está deshabilitada de forma predeterminada.

8. Si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.

9. Haga clic en el botón **Finalizar**.

   Se crea la tarea y se la agrega a la lista de tareas.

10. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.

11. En la ventana de propiedades de la tarea, modifique los ajustes generales de la tarea según resulte necesario.

12. Haga clic en el botón **Guardar**.

    La tarea queda creada y configurada.

Si los resultados de la tarea contienen una advertencia del error 0x80240033 "Error del Agente de Windows Update 80240033 (" No se pudieron descargar los términos de licencia "), puede resolver este problema a través del Registro de Windows .

## Agregar reglas de instalación de actualizaciones

Esta función solo está disponible con una licencia de Administración de vulnerabilidades y parches.

Si desea utilizar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para instalar actualizaciones de software o reparar vulnerabilidades en sus aplicaciones, debe definir reglas de instalación de actualizaciones. Estas reglas determinan qué actualizaciones se deben instalar y qué vulnerabilidades se deben reparar.

La configuración exacta depende de si la regla se crea para todas las actualizaciones, para actualizaciones de Windows Update o para actualizaciones publicadas para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky y Microsoft). Cuando agregue una regla para actualizaciones de Windows Update o para actualizaciones de aplicaciones de terceros, podrá seleccionar las aplicaciones específicas (y las versiones puntuales de esas aplicaciones) para las que quiera instalar actualizaciones. Cuando agregue una regla para todas las actualizaciones, podrá seleccionar las actualizaciones específicas que quiera instalar y las vulnerabilidades puntuales que quiera reparar mediante la instalación de actualizaciones.

Para agregar una regla de instalación de actualizaciones, puede optar por cualquiera de estos métodos:

- Agregue la regla cuando esté creando una nueva tarea Instalar actualizaciones requeridas y reparar vulnerabilidades.
- Agregue la regla en la pestaña **Configuración de la aplicación** de la ventana de propiedades de una tarea de *Instalar actualizaciones requeridas y reparar vulnerabilidades*.
- Utilice el Asistente de instalación de actualizaciones o el Asistente de reparación de vulnerabilidades.

*Para agregar una nueva regla para todas las actualizaciones, haga lo siguiente:*

1. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Siguiente**.

2. En la página **Tipo de regla**, seleccione **Regla para todas las actualizaciones**.

3. En la página **Criterios generales**, use las listas desplegables para definir los siguientes ajustes:

   - **Conjunto de actualizaciones para instalar**

     Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

     - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

   - **Reparar vulnerabilidades que tengan o superen este nivel de gravedad**

     Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

     Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

     Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

     Esta opción está deshabilitada de forma predeterminada.

4. En la página **Actualizaciones**, seleccione las actualizaciones que se instalarán:

   - **Instalar todas las actualizaciones adecuadas**

     Se instalarán todas las actualizaciones de software que cumplan con los criterios especificados en la página **Criterios generales** del asistente. Esta es la opción seleccionada por defecto.

   - **Instalar solo las actualizaciones de la lista**

     Se instalarán únicamente las actualizaciones de software que seleccione manualmente en la lista. La lista contiene todas las actualizaciones de software disponibles.

     Existen situaciones en las que querrá elegir manualmente las actualizaciones que se instalarán: podría suceder, por ejemplo, que quiera evaluar ciertas actualizaciones en un entorno de prueba, que quiera actualizar solo las aplicaciones que considere importantes o que necesite actualizar solo algunas aplicaciones puntuales.

     - **Instalar automáticamente todas las actualizaciones de aplicaciones previas requeridas para instalar las actualizaciones seleccionadas**

       Mantenga habilitada esta opción si está de acuerdo en que, para instalar las actualizaciones seleccionadas, se instalen versiones intermedias de las aplicaciones.

       Si deshabilita esta opción, se instalarán únicamente las versiones de las aplicaciones que haya seleccionado. Deshabilite esta opción si quiere que las aplicaciones se actualicen en forma directa, sin que se trate de instalar versiones intermedias. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

       A modo de ejemplo, imagine que un dispositivo tiene instalada la versión 3 de una aplicación. Quiere actualizar esa versión a la 5, pero la versión 5 solo se puede instalar sobre la versión 4. Si esta opción está habilitada, el software instalará primero la versión 4 y luego la versión 5. Si esta opción está deshabilitada, el software no podrá actualizar la aplicación.

       Esta opción está activada de forma predeterminada.

5. En la página **Vulnerabilidades**, seleccione las vulnerabilidades que se repararán al instalar las actualizaciones seleccionadas:

   - **Reparar todas las vulnerabilidades que coincidan con otros criterios**

     Se repararán todas las vulnerabilidades que cumplan con los criterios especificados en la página **Criterios generales** del asistente. Esta es la opción seleccionada por defecto.

   - **Reparar solo las vulnerabilidades de la lista**

     Se repararán únicamente las vulnerabilidades que seleccione manualmente en la lista. La lista contiene todas las vulnerabilidades detectadas.

     Existen situaciones en las que querrá elegir manualmente las vulnerabilidades que se repararán: podría suceder, por ejemplo, que quiera verificar en un entorno de prueba que las vulnerabilidades se puedan reparar, que quiera reparar las vulnerabilidades solo en las aplicaciones que considere importantes o que prefiera reparar las vulnerabilidades solo en ciertas aplicaciones puntuales.

6. En la página **Nombre**, escriba un nombre para la regla que está agregando. Podrá cambiar este nombre más tarde, en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Cuando el Asistente de creación de reglas llegue a su fin, se agregará la nueva regla. La encontrará en la lista de reglas del Asistente para crear nueva tarea o en las propiedades de la tarea.

*Para agregar una nueva regla para actualizaciones de Windows Update, haga lo siguiente:*

1. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Siguiente**.

2. En la página **Tipo de regla**, seleccione **Regla para Windows Update**.

3. En la página **Criterios generales**, defina los siguientes ajustes:

- Conjunto de actualizaciones para instalar

  Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

  - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
  - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
  - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

- Reparar vulnerabilidades que tengan o superen este nivel de gravedad

  Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

  Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

  Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

  Esta opción está deshabilitada de forma predeterminada.

- Reparar vulnerabilidades con un nivel de gravedad de MSRC igual o mayor que

  Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

  Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que el Centro de respuestas de seguridad de Microsoft (MSRC) haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

  Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

  Esta opción está deshabilitada de forma predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desee instalar actualizaciones. Por defecto, están seleccionadas todas las aplicaciones.

5. En la página **Categorías de actualizaciones**, seleccione las categorías de actualizaciones que se instalarán. Las categorías son las mismas que se usan en el Catálogo de Microsoft Update. Por defecto, están seleccionadas todas las categorías.

6. En la página **Nombre**, escriba un nombre para la regla que está agregando. Podrá cambiar este nombre más tarde, en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Cuando el Asistente de creación de reglas llegue a su fin, se agregará la nueva regla. La encontrará en la lista de reglas del Asistente para crear nueva tarea o en las propiedades de la tarea.

*Para agregar una nueva regla para actualizaciones de aplicaciones de terceros, haga lo siguiente:*

1. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Siguiente**.

2. En la página **Tipo de regla**, seleccione **Regla para las actualizaciones de terceros**.

3. En la página **Criterios generales**, defina los siguientes ajustes:

   - Conjunto de actualizaciones para instalar

     Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

     - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

   - Reparar vulnerabilidades que tengan o superen este nivel de gravedad

     Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

     Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

     Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

     Esta opción está deshabilitada de forma predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desee instalar actualizaciones. Por defecto, están seleccionadas todas las aplicaciones.

5. En la página **Nombre**, escriba un nombre para la regla que está agregando. Podrá cambiar este nombre más tarde, en la sección Configuración de la ventana de propiedades de la tarea creada.

Cuando el Asistente de creación de reglas llegue a su fin, se agregará la nueva regla. La encontrará en la lista de reglas del Asistente para crear nueva tarea o en las propiedades de la tarea.

## Selección de soluciones de usuario para vulnerabilidades de software de terceros

Para usar la tarea *Reparar vulnerabilidades*, debe especificar manualmente las actualizaciones de software para reparar las vulnerabilidades en el software de terceros que se detalla en la configuración de la tarea. La tarea *Reparar vulnerabilidades* utiliza reparaciones recomendadas para el software de Microsoft y reparaciones de usuario para otro software de terceros. Las *correcciones de usuario* son actualizaciones de software para reparar vulnerabilidades que el administrador especifica manualmente para la instalación.

*Para seleccionar reparaciones de usuario para vulnerabilidades en software de terceros, realice lo siguiente:*

1. En el menú principal, vaya a **Operaciones → Administración de parches → Vulnerabilidades de software**.

   La página muestra la lista de vulnerabilidades de software detectadas en los dispositivos cliente.

2. En la lista de vulnerabilidades de software, haga clic en el vínculo con el nombre de la vulnerabilidad de software para la que desea especificar una reparación del usuario.

   Se abre la ventana de propiedades de la vulnerabilidad.

3. En el panel de la izquierda, seleccione la sección **Correcciones del usuario y otras correcciones**.

   Se muestra la lista de reparaciones del usuario para la vulnerabilidad de software seleccionada.

4. Haga clic en **Agregar**.

   Se muestra una lista de paquetes de instalación disponibles. La lista de paquetes de instalación que se muestran corresponde a la lista **Operaciones → Repositorios → Paquetes de instalación**. Si no ha creado un paquete de instalación que contenga la reparación del usuario para la vulnerabilidad seleccionada, ahora puede crear el paquete iniciando el Asistente de nuevo paquete.

5. Seleccione uno o más paquetes de instalación que contengan una o más reparaciones del usuario para la vulnerabilidad en el software de terceros.

6. Haga clic en **Guardar**.

Se especifican los paquetes de instalación que contienen reparaciones de usuario para la vulnerabilidad de software. Cuando se inicie la tarea *Reparar vulnerabilidades*, se instalará el paquete de instalación y se reparará la vulnerabilidad de software.

## Ver información sobre las vulnerabilidades de software detectadas en todos los dispositivos administrados

Si ya ha analizado el software de los dispositivos administrados en busca de vulnerabilidades, puede ver la lista de vulnerabilidades de software detectadas en la totalidad de los dispositivos administrados. Si ejecuta la tarea para la jerarquía de Servidores de administración, puede ver la lista de dispositivos administrados con vulnerabilidades detectadas solo para el Servidor de administración seleccionado.

*Para ver la lista de vulnerabilidades de software detectadas en todos los dispositivos administrados:*

En el menú principal, vaya a **Operaciones → Administración de parches → Vulnerabilidades de software**.

La página muestra la lista de vulnerabilidades de software detectadas en los dispositivos cliente.

También puede generar y ver un informe de vulnerabilidades.

Puede aplicar un filtro para ver la lista de vulnerabilidades de software. Para definir el filtro, haga clic en el ícono **Filtrar** (⚙) ubicado en la esquina superior derecha de la lista de vulnerabilidades de software. También puede elegir un filtro preestablecido de la lista desplegable **Filtros preestablecidos**, que se encuentra sobre la lista de vulnerabilidades de software.

Si lo desea, puede obtener información detallada sobre cualquiera de las vulnerabilidades de la lista.

*Para obtener información sobre una vulnerabilidad de software:*

En la lista de vulnerabilidades de software, haga clic en el vínculo con el nombre de la vulnerabilidad de su interés.

Se abre la ventana de propiedades de la vulnerabilidad de software.

## Ver información sobre las vulnerabilidades de software detectadas en un dispositivo administrado específico

Puede ver información sobre las vulnerabilidades de software detectadas en un dispositivo administrado específico que ejecute Windows.

*Para ver la lista de las vulnerabilidades de software detectadas en el dispositivo administrado seleccionado:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo para el que desee ver las vulnerabilidades de software detectadas.

   Se muestra la ventana de propiedades del dispositivo seleccionado.

3. En la ventana de propiedades del dispositivo seleccionado, elija la pestaña **Avanzado**.

4. En el panel izquierdo, seleccione la sección **Vulnerabilidades de software**.

Se muestra la lista de vulnerabilidades de software detectadas en el dispositivo administrado que seleccionó.

*Para ver las propiedades de una vulnerabilidad de software específica:*

En la lista de vulnerabilidades de software, haga clic en el vínculo con el nombre de la vulnerabilidad de software que sea de su interés.

Se muestra la ventana de propiedades de la vulnerabilidad de software seleccionada.

# Ver estadísticas de las vulnerabilidades presentes en los dispositivos administrados

Puede ver estadísticas sobre cada vulnerabilidad de software detectada en los dispositivos administrados. Las estadísticas se presentan en forma de diagrama. El diagrama muestra la cantidad de dispositivos con los siguientes estados:

- *Ignorada en: <cantidad de dispositivos>*. Este estado se asigna cuando la vulnerabilidad se desestima manualmente a través de sus propiedades.
- *Reparada en: <cantidad de dispositivos>*. Este estado se asigna cuando la tarea para reparar la vulnerabilidad se completa correctamente.
- *Reparación programada para: <cantidad de dispositivos>*. Este estado se asigna cuando ya se ha creado una tarea para reparar la vulnerabilidad, pero aún no se la ha ejecutado.
- *Parche aplicado en: <cantidad de dispositivos>*. Este estado se asigna cuando se seleccionó manualmente una actualización de software que debía, pero no pudo, reparar la vulnerabilidad.
- *Es necesario realizar un arreglo en: <cantidad de dispositivos>*. Este estado se asigna cuando la vulnerabilidad se ha reparado solo en algunos dispositivos administrados y aún debe repararse en más dispositivos administrados.

*Para ver las estadísticas de una vulnerabilidad en los dispositivos administrados:*

1. En el menú principal, vaya a **Operaciones → Administración de parches → Vulnerabilidades de software**.

   La página muestra una lista con las vulnerabilidades detectadas en las aplicaciones de los dispositivos administrados.

2. Active la casilla de verificación ubicada junto a la vulnerabilidad de su interés.

3. Haga clic en el botón **Estadísticas de la vulnerabilidad en los dispositivos**.

Se muestra un diagrama con los estados de la vulnerabilidad. Para ver los dispositivos en los que la vulnerabilidad tenga un estado en particular, haga clic en ese estado.

# Exportar la lista de vulnerabilidades de software a un archivo

Puede exportar la lista de vulnerabilidades que se muestra en la aplicación a un archivo CSV o TXT. Una vez que tenga el archivo, podrá almacenarlo para fines estadísticos, enviarlo a la persona que esté a cargo de la seguridad de la información o utilizarlo para otros fines.

*Para exportar a un archivo de texto la lista de vulnerabilidades de software detectadas en todos los dispositivos administrados:*

1. En el menú principal, vaya a **Operaciones → Administración de parches → Vulnerabilidades de software**.

   La página muestra una lista con las vulnerabilidades detectadas en las aplicaciones de los dispositivos administrados.

2. Haga clic en el botón **Exportar a TXT** o en el botón **Exportar a CSV**, dependiendo del formato de exportación que prefiera.

El archivo con la lista de vulnerabilidades de software se guardará en el dispositivo que esté utilizando.

*Para exportar a un archivo de texto la lista de vulnerabilidades de software detectadas en un dispositivo administrado específico:*

1. Abra la lista de vulnerabilidades de software detectadas en el dispositivo administrado de su interés.
2. Seleccione las vulnerabilidades de software que desee exportar.

   Omita este paso si desea exportar toda la lista de vulnerabilidades de software detectadas en el dispositivo administrado.

   Si desea exportar la lista completa de vulnerabilidades de software detectadas en el dispositivo administrado, tenga en cuenta que solo se exportarán las vulnerabilidades enumeradas en la página que esté viendo.
3. Haga clic en el botón **Exportar a TXT** o en el botón **Exportar a CSV**, dependiendo del formato de exportación que prefiera.

En el dispositivo que esté utilizando, se guardará un archivo con la lista de vulnerabilidades de software detectadas en el dispositivo administrado que haya seleccionado.

## Ignorar vulnerabilidades de software

Puede ignorar las vulnerabilidades de software que no desee reparar. Hay distintos motivos para ignorar una vulnerabilidad de software, por ejemplo:

- no considera que la vulnerabilidad de software sea de extrema importancia para su organización;
- entiende que, al reparar la vulnerabilidad, se pondrían en riesgo los datos vinculados al software vulnerable;
- sabe que la vulnerabilidad de software no es un riesgo para la red de su organización porque utiliza otras medidas para proteger sus dispositivos administrados.

Puede ignorar una vulnerabilidad de software en todos los dispositivos administrados o solo en los dispositivos administrados que usted seleccione.

*Para ignorar una vulnerabilidad de software en todos los dispositivos administrados:*

1. En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Vulnerabilidades de software**.

   La página muestra una lista con las vulnerabilidades de software detectadas en los dispositivos administrados.
2. En la lista de vulnerabilidades de software, haga clic en el vínculo con el nombre de la vulnerabilidad de software que desee ignorar.

   Se abre la ventana de propiedades de la vulnerabilidad de software.
3. En la pestaña **General**, habilite la opción **Ignorar vulnerabilidad**.
4. Haga clic en el botón **Guardar**.

   Se cierra la ventana de propiedades de la vulnerabilidad de software.

La vulnerabilidad de software se ignorará en todos los dispositivos administrados.

*Para ignorar una vulnerabilidad de software en un dispositivo administrado específico:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo en el que desee ignorar la vulnerabilidad de software.

   Se abre la ventana de propiedades del dispositivo.

3. En la ventana de propiedades del dispositivo, seleccione la pestaña **Avanzado**.

4. En el panel izquierdo, seleccione la sección **Vulnerabilidades de software**.

   Se muestra la lista de vulnerabilidades de software detectadas en el dispositivo.

5. En la lista de vulnerabilidades de software, seleccione la vulnerabilidad que desee ignorar en el dispositivo seleccionado.

   Se abre la ventana de propiedades de la vulnerabilidad de software.

6. En la ventana de propiedades de la vulnerabilidad de software, en la pestaña **General**, habilite la opción **Ignorar vulnerabilidad**.

7. Haga clic en el botón **Guardar**.

   Se cierra la ventana de propiedades de la vulnerabilidad de software.

8. Cierre la ventana de propiedades del dispositivo.

La vulnerabilidad de software se ignorará en el dispositivo seleccionado.

Cuando se completen las tareas *Reparar vulnerabilidades* o *Instalar actualizaciones requeridas y reparar vulnerabilidades*, las vulnerabilidades de software ignoradas no se repararán. Las vulnerabilidades ignoradas pueden excluirse de la lista de vulnerabilidades utilizando un filtro.

# Administración de las aplicaciones que se ejecutan en los dispositivos cliente

En esta sección se describen las funciones de Kaspersky Security Center relacionadas con la administración de las aplicaciones que se ejecutan en los dispositivos cliente.

## Uso de Control de aplicaciones para administrar archivos ejecutables

Puede utilizar el componente Control de aplicaciones para permitir o bloquear el inicio de archivos ejecutables en los dispositivos del usuario. El componente Control de aplicaciones es compatible con sistemas operativos Windows y Linux.

Para los sistemas operativos Linux, el componente Control de aplicaciones está disponible a partir de Kaspersky Endpoint Security 11.2 para Linux. El componente también está disponible para Kaspersky Embedded Systems Security para Windows 3.0 o posterior.

## Requisitos previos

- Kaspersky Security Center está desplegado en su organización.
- Se ha creado y activado una directiva para Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security para Windows.
- La directiva de Kaspersky Embedded Systems Security for Windows o Kaspersky Embedded Systems Security for Linux ahora está creada y activa.

## Etapas

El procedimiento de uso de Control de aplicaciones consta de etapas:

1. **Crear y ver la lista de archivos ejecutables almacenados en los dispositivos cliente**

   En esta etapa, podrá descubrir qué archivos ejecutables se encuentran guardados en los dispositivos administrados. Revise la lista de archivos ejecutables y compárela con las listas de archivos ejecutables permitidos y prohibidos. Las restricciones sobre el uso de archivos ejecutables pueden estar vinculadas a las políticas de seguridad de la información de su organización.

   Instrucciones:

   - Consola de administración: inventario de archivos ejecutables
   - Kaspersky Security Center Web Console: obtención y visualización de una lista de archivos ejecutables almacenados en los dispositivos cliente

2. **Creación de categorías para archivos ejecutables utilizados en la organización**

   Analice las listas de aplicaciones y archivos ejecutables almacenados en los dispositivos administrados. Cree las categorías para archivos ejecutables en función del análisis. Recomendamos crear una categoría llamada "Aplicaciones de trabajo" que cubra los archivos ejecutables estándar que se utilicen en la organización. Luego, si tiene grupos de seguridad diferentes que trabajan con sus propios archivos ejecutables, puede crear una categoría independiente para cada grupo de seguridad.

   Instrucciones:

   - Consola de administración: Creación de una categoría de aplicaciones con contenido agregado manualmente, Creación de una categoría de aplicaciones que incluya archivos ejecutables de dispositivos seleccionados, Creación de una categoría de aplicaciones que incluya archivos ejecutables de una carpeta específica.
   - Kaspersky Security Center Web Console: Creación de una categoría de aplicaciones con contenido agregado manualmente, Creación de una categoría de aplicaciones que incluya archivos ejecutables de dispositivos seleccionados, Creación de una categoría de aplicaciones que incluya archivos ejecutables de una carpeta seleccionada.

3. **Configurar Control de aplicaciones en la directiva de Kaspersky Endpoint Security**

   Configure el componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security utilizando las categorías que creó en la etapa anterior.

   Instrucciones:

   - Consola de administración: Configuración de la administración de inicio de aplicaciones en dispositivos cliente

- Kaspersky Security Center Web Console: Configuración del Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows

4. **Configurar el Control de aplicaciones en la directiva de aplicaciones de Kaspersky Embedded Systems Security**

   Configure el componente Control de aplicaciones en la directiva de Kaspersky Embedded Systems Security para Windows utilizando las categorías que ha creado. Para obtener más información sobre el componente Control de aplicaciones, consulte la Ayuda de Kaspersky Embedded Systems Security para Windows o la Ayuda de Kaspersky Embedded Systems Security para Linux.

   Si utiliza una gran cantidad de reglas, puede producirse un error al cargar la directiva. Puede aumentar el tamaño máximo de solicitud en bytes utilizando los siguientes comandos:

   - Para la solicitud JSON:

     ```
     klscflag -fset -pv ".core/.independent" -s KLLIM -n
     LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v <max_request_size> -t d
     ```

   - Para la solicitud HTTP:

     ```
     klscflag -fset -pv ".core/.independent" -s KLLIM -n
     LP_KLOAPI_MaxSizeOfHttpRequestInBytes -v <max_request_size> -t d
     ```

     Dónde `<max_request_size>` es el tamaño máximo de solicitud en bytes (por ejemplo, `200000000`).

5. **Activar el componente Control de aplicaciones en modo de prueba**

   Las reglas de Control de aplicaciones no deben bloquear los archivos ejecutables que los usuarios necesiten para trabajar. Para asegurarse de que esto sea así, cuando cree nuevas reglas de Control de aplicaciones, recomendamos que habilite un modo de prueba y analice el funcionamiento de las reglas. Mientras estas pruebas se encuentren activas, Kaspersky Endpoint Security para Windows o Kaspersky Embedded Systems Security no bloqueará los archivos ejecutables que las reglas de Control de aplicaciones no permitan iniciar, sino que simplemente notificará al Servidor de administración para informar de que tales aplicaciones se han iniciado.

   Para probar las reglas de Control de aplicaciones, recomendamos que haga lo siguiente:

   - Defina la duración del período de prueba. El período de prueba puede durar de varios días a dos meses.
   - Examine los eventos que surjan de probar el funcionamiento de Control de aplicaciones.

   Instrucciones para Kaspersky Security Center Web Console: Configuración del componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows. Siga estas instrucciones y habilite la opción **Modo de prueba** en el proceso de configuración.

6. **Cambiar la configuración de las categorías en el componente Control de aplicaciones**

   De ser necesario, modifique la configuración de Control de aplicaciones. Con los resultados de las pruebas, puede crear una categoría con contenido agregado manualmente que incluya los archivos ejecutables vinculados a los eventos de Control de aplicaciones.

   Instrucciones:

   - Consola de administración: Adición de archivos ejecutables relacionados con un evento a una categoría de aplicaciones
   - Kaspersky Security Center Web Console: Adición de archivos ejecutables relacionados con un evento a una categoría de aplicaciones

7. **Aplicar las reglas de Control de aplicaciones en modo de funcionamiento normal**

   Después de probar las reglas de Control de aplicaciones y completar la configuración de las categorías, podrá aplicar las reglas de Control de aplicaciones en el modo de operación.

Instrucciones para Kaspersky Security Center Web Console: Configuración del componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows. Siga estas instrucciones y deshabilite la opción **Modo de prueba** en el proceso de configuración.

8. **Verificar la configuración de Control de aplicaciones**

   Asegúrese de haber hecho lo siguiente:

   - Categorías de archivos ejecutables creadas.
   - Configuración de Control de aplicaciones con las categorías.
   - Aplicar las reglas de Control de aplicaciones en el modo de operación.

## Resultados

Al concluir este procedimiento, el inicio de archivos ejecutables en los dispositivos administrados estará bajo su control. Los usuarios pueden iniciar solo aquellos archivos ejecutables que están permitidos en su organización y no pueden iniciar los que están prohibidos.

Para obtener información detallada sobre el Control de aplicaciones, consulte los siguientes temas de ayuda:

- Ayuda en línea de Kaspersky Endpoint Security para Windows
- Ayuda en línea de Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Ayuda de Kaspersky Embedded Systems Security para Windows
- Ayuda de Kaspersky Embedded Systems Security para Linux

## Modos y categorías de Control de aplicaciones

El componente Control de aplicaciones supervisa los intentos de los usuarios de iniciar archivos ejecutables. Puede usar las reglas de Control de aplicaciones para controlar el inicio de archivos ejecutables.

> El componente Control de aplicaciones está disponible en Kaspersky Endpoint Security para Windows, Kaspersky Endpoint Security 11.2 for Linux y versiones posteriores, y Kaspersky Security for Virtualization Light Agent. Todas las instrucciones de esta sección describen la configuración de Control de aplicaciones para Kaspersky Endpoint Security para Windows.

El inicio de archivos ejecutables cuya configuración no coincide con ninguna de las reglas de Control de aplicaciones está regulado por el modo de funcionamiento seleccionado del componente:

- *Lista de rechazados*. En este modo, se permite la ejecución de cualquier archivo ejecutable, excepto los que se especifican en las reglas de bloqueo. Este modo está seleccionado de forma predeterminada.
- *Lista de admitidos*. En este modo, se impide la ejecución de todos los archivos ejecutables, excepto los que se especifican en las reglas de autorización.

Las reglas de Control de aplicaciones se implementan en todas las categorías de archivos ejecutables. En Kaspersky Security Center, hay tres tipos de categorías:

- Categorías con contenido agregado de forma manual. Para sumar archivos ejecutables a una categoría de este tipo, deberá definir distintas condiciones: metadatos del archivo, código hash del archivo, certificado del archivo, categoría KL, ruta de acceso al archivo, etc.
- Categoría que incluye los archivos ejecutables de los dispositivos seleccionados. Para crear una categoría de este tipo, deberá seleccionar un dispositivo. Los archivos ejecutables de ese dispositivo se agregarán a la categoría automáticamente.
- Categoría que incluye archivos ejecutables de la carpeta seleccionada. Especifica una carpeta cuyos archivos ejecutables se incluirán automáticamente dentro de la categoría.

Para obtener información detallada sobre el Control de aplicaciones, consulte los siguientes temas de ayuda:

- Ayuda en línea de Kaspersky Endpoint Security para Windows
- Ayuda en línea de Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Ayuda de Kaspersky Embedded Systems Security para Windows
- Ayuda de Kaspersky Embedded Systems Security para Linux

## Obtención y visualización de una lista de archivos ejecutables almacenados en los dispositivos cliente

Puede obtener la lista de archivos ejecutables almacenados en los dispositivos cliente de una de las siguientes maneras:

- Habilitando las notificaciones sobre el inicio de aplicaciones en la directiva de Kaspersky Endpoint Security.
- Creando una tarea de inventario.

## Habilitando las notificaciones sobre el inicio de aplicaciones en la directiva de Kaspersky Endpoint Security

*Para habilitar las notificaciones sobre la ejecución de aplicaciones:*

1. Abra la configuración de la directiva de Kaspersky Endpoint Security y luego vaya a **Configuración general** → **Informes y almacenamiento**.
2. En el grupo de configuración **Transferencia de datos al servidor de administración**, seleccione la casilla de verificación **Acerca de las aplicaciones iniciadas** y guarde los cambios.

Cuando un usuario intenta iniciar archivos ejecutables, la información sobre estos archivos se añade a la lista de archivos ejecutables en el dispositivo cliente. Kaspersky Endpoint Security envía esta información al Agente de red, que a su vez la envía al Servidor de administración.

## Crear una tarea de inventario

La función de inventario de archivos ejecutables está disponible para las siguientes aplicaciones:

- Kaspersky Endpoint Security para Windows
- Kaspersky Endpoint Security for Linux (versión 11.2 y posteriores)
- Kaspersky Security for Virtualization 4.0 Light Agent y versiones posteriores

Puede reducir la carga a la que se somete la base de datos cuando se obtiene información sobre las aplicaciones instaladas. Para ahorrar espacio en la base de datos, recomendamos que ejecute una tarea de inventario en los dispositivos de referencia que tengan instalada una selección de aplicaciones estándar. El número preferible de dispositivos es de 1 a 3.

Desaconsejamos ejecutar la tarea de inventario si se utilizan las siguientes bases de datos: MySQL, PostgreSQL, SQL Server Express Edition, MariaDB (cualquier edición).

*Para crear una tarea que haga un inventario de los archivos ejecutables instalados en los dispositivos cliente:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.

   Se muestra la lista de tareas.

2. Haga clic en el botón **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.

3. En la página **Configuración de tarea nueva**, en la lista desplegable **Aplicación**, elija Kaspersky Endpoint Security para Windows o Kaspersky Endpoint Security for Linux, según el tipo de sistema operativo de los dispositivos cliente.

4. En la lista desplegable **Tipo de tarea**, seleccione **Inventario**.

5. En la página **Finalizar la creación de la tarea**, haga clic en el botón **Finalizar**.

   Una vez que finalice el Asistente para crear nueva tarea, se creará y configurará la tarea **Inventario**. Si lo desea, puede cambiar la configuración de la tarea creada. Encontrará la nueva tarea en la lista de tareas.

Para obtener una descripción detallada de la tarea de inventario, consulte las siguientes ayudas:

- Ayuda de Kaspersky Endpoint Security para Windows
- Ayuda de Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Una vez efectuada la tarea **Inventario**, se crea la lista de archivos ejecutables almacenados en los dispositivos administrados para que pueda verla.

Durante el inventario, se pueden detectar archivos ejecutables en los siguientes formatos (dependiendo de la opción que seleccione en las propiedades de la tarea de inventario): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR y HTML.

## Consultar las listas de archivos ejecutables almacenados en los dispositivos administrados

*Para visualizar la lista de los archivos ejecutables almacenados en los dispositivos cliente, haga lo siguiente:*

En el menú principal, vaya a **Operaciones** → **Aplicaciones de terceros** → **Archivos ejecutables**.

La página muestra la lista de los archivos ejecutables almacenados en los dispositivos cliente.

Si es necesario, puede enviar el archivo ejecutable del dispositivo administrado al dispositivo donde está abierta su Kaspersky Security Center Web Console.

*Para enviar un archivo ejecutable:*

1. En el menú principal, vaya a **Operaciones** → **Aplicaciones de terceros** → **Archivos ejecutables**.
2. Haga clic en el enlace del archivo ejecutable que desea enviar.
3. En la ventana que se abre, vaya a **Dispositivos** y seleccione la casilla del dispositivo administrado desde el que desea enviar el archivo ejecutable.

   Antes de enviar el archivo ejecutable, marque la casilla **No desconectar del Servidor de administración** para asegurarse de que el dispositivo administrado tenga una conexión directa con el Servidor de administración.

4. Haga clic en el botón **Enviar**.

   El archivo ejecutable seleccionado se descarga para su posterior envío al dispositivo donde está abierta Kaspersky Security Center Web Console.

## Crear una categoría de aplicaciones con contenido agregado manualmente

Puede especificar un conjunto de criterios que sean comunes a los archivos ejecutables que los usuarios podrán o no podrán iniciar en su organización. Puede agregar los archivos que respondan a estos criterios a una nueva categoría de aplicaciones. Más tarde, podrá usar esa nueva categoría para configurar el componente Control de aplicaciones.

*Para crear una categoría de aplicaciones con contenido agregado manualmente:*

1. En el menú principal, vaya a **Operaciones** → **Aplicaciones de terceros** → **Categorías de aplicaciones**.

   Se muestra una página con una lista de categorías de aplicaciones.

2. Haga clic en el botón **Agregar**.

   Se inicia el Asistente para crear nueva categoría. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. En el paso **Seleccione un método para crear la categoría**, seleccione la opción **Categoría con contenido agregado de forma manual. Los datos de los archivos ejecutables se agregan de forma manual a la categoría**.

4. En el paso **Condiciones**, haga clic en el botón **Agregar** para agregar un criterio de condición e incluir archivos en la categoría de creación.

5. En el paso **Criterios de la condición**, seleccione el tipo de regla que desee usar para crear la categoría:

- **De la categoría KL**

  Seleccione esta opción si, como condición para agregar aplicaciones a la categoría personalizada, desea elegir una categoría de aplicaciones de Kaspersky. Las aplicaciones que pertenezcan a la categoría de Kaspersky elegida se agregarán a la categoría de aplicaciones personalizada.

- **Seleccionar el certificado del repositorio**

  Seleccione esta opción para elegir certificados almacenados en el repositorio. La condición de la categoría solo coincide con los archivos ejecutables que están firmados por el certificado especificado.

  Los certificados se agregan al repositorio si creó e inició una tarea de inventario o marcó la casilla **Acerca de las aplicaciones iniciadas** en la directiva de Kaspersky Endpoint Security. Puede realizar ambas acciones.

- **Especificar la ruta a la aplicación (se pueden usar máscaras)**

  Seleccione esta opción para especificar la ruta a un archivo o carpeta del dispositivo cliente que contenga los archivos ejecutables que quiera agregar a la categoría de aplicaciones personalizada. Puede utilizar expresiones regulares como *C:\path_to_exe*.*, por ejemplo: *C:\Program Files\Internet Explorer*.*

- **Unidad extraíble**

  Seleccione esta opción para especificar el tipo de soporte (unidad extraíble o cualquier tipo de unidad) desde el que se ejecuta la aplicación. Las aplicaciones que se inicien desde el tipo de unidad seleccionado se agregarán a la categoría de aplicaciones personalizada.

- **Hash, metadatos o certificado**:

  - **Seleccionar de la lista de archivos ejecutables**

    Seleccione esta opción si desea elegir las aplicaciones que se agregarán a la categoría de la lista de archivos ejecutables almacenados en el dispositivo cliente.

  - **Seleccionar del registro de aplicaciones**

Si selecciona esta opción, se abrirá el registro de aplicaciones. Después de seleccionar una aplicación del registro, se abre la ventana con los parámetros llenos de metadatos de la aplicación que seleccionó:

- Nombre del archivo.
- Versión del archivo. Puede indicar el número de versión exacto o introducir una condición, como "superior a 5.0".
- Nombre de la aplicación.
- Versión de la aplicación. Puede indicar el número de versión exacto o introducir una condición, como "superior a 5.0".
- Proveedor.

Tenga en cuenta que solo se bloquea la ejecución de archivos ejecutables que cumplan con los parámetros especificados, no la ejecución de la aplicación que seleccione. Si los metadatos de la aplicación seleccionada coinciden con el del archivo ejecutable que se ejecuta al iniciar la aplicación, puede continuar con el siguiente paso. De lo contrario, debe cambiar los valores manualmente para que coincidan con los metadatos del archivo ejecutable.

- **Especificar manualmente**

Selecciona esta opción para especificar los metadatos, el certificado o el hash de archivo que se tomarán como condición para agregar aplicaciones a la categoría personalizada.

**Hash de archivo**

Según la versión de la aplicación de seguridad instalada en los dispositivos en su red, debe seleccionar un algoritmo para que Kaspersky Security Center calcule el valor de hash para archivos en esta categoría. La información sobre los valores hash calculados por las funciones hash se almacena en la base de datos del Servidor de administración.

SHA256 es una función de hash criptográfica. En la actualidad, se la considera la más confiable en su clase, pues no se encontró vulnerabilidad alguna en su algoritmo. Kaspersky Endpoint Security puede calcular hashes SHA256 desde la versión 10 Service Pack 2 para Windows. Las versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows son compatibles con la función de hash MD5.

Seleccione cualquiera de las opciones de evaluación del valor de hash de Kaspersky Security Center para archivos en la categoría:

- Si todas las instancias de aplicaciones de seguridad instaladas en su red son Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores, marque la casilla **SHA256**. Si hay versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows en su red, recomendamos que no agregue categorías que utilicen como criterio el hash SHA256 del archivo ejecutable. Si lo hace, la aplicación de seguridad podría no funcionar correctamente. De presentarse inconvenientes, utilice la función de hash criptográfico MD5 para los archivos de la categoría.

- Si hay alguna versión anterior a Kaspersky Endpoint Security 10 Service Pack 2 para Windows instalada en su red, seleccione **Hash MD5**. No puede agregar una categoría que se haya creado según el criterio de la suma de verificación MD5 de un archivo ejecutable para Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores. De presentarse inconvenientes, utilice la función de hash criptográfico SHA256 para los archivos de la categoría.

- Si diferentes dispositivos en su red usan versiones anteriores y posteriores de Kaspersky Endpoint Security 10, marque la casilla **SHA256** y la casilla **Hash MD5**.

**Metadatos**

Seleccione esta opción si desea especificar los metadatos de los archivos (nombre, versión, proveedor, etc.). La condición de la categoría solo coincide con los archivos ejecutables que tienen los mismos metadatos.

**Certificado**

Seleccione esta opción para elegir certificados almacenados en el repositorio. La condición de la categoría solo coincide con los archivos ejecutables que están firmados por el certificado especificado.

Los certificados se agregan al repositorio si creó e inició una tarea de inventario o marcó la casilla **Acerca de las aplicaciones iniciadas** en la directiva de Kaspersky Endpoint Security. Puede realizar ambas acciones.

- **Desde archivo o paquete MSI/carpeta archivada**

  Seleccione esta opción para especificar un archivo de instalador MSI como condición para agregar aplicaciones a la categoría personalizada. Los metadatos del instalador se enviarán al Servidor de administración. Las aplicaciones que tengan los mismos metadatos de instalador que el instalador MSI especificado se agregarán a la categoría de aplicaciones personalizada.

El criterio seleccionado se agrega a la lista de condiciones.

Puede agregar tantos criterios como necesite para crear la categoría de aplicaciones.

6. En el paso **Exclusiones**, haga clic en el botón **Agregar** para agregar un criterio de condición excluyente que permita excluir archivos de la nueva categoría.

7. En el paso **Criterios de la condición**, seleccione un tipo de regla tal como lo hizo al elegir un tipo de regla para crear la categoría.

Cuando el asistente finaliza, se crea la categoría de aplicaciones. La nueva categoría aparece en la lista de categorías de aplicaciones. Podrá usar la nueva categoría cuando configure Control de aplicaciones.

Para obtener información detallada sobre el Control de aplicaciones, consulte los siguientes temas de ayuda:

- Ayuda en línea de Kaspersky Endpoint Security para Windows
- Ayuda en línea de Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Ayuda de Kaspersky Embedded Systems Security para Windows
- Ayuda de Kaspersky Embedded Systems Security para Linux

## Crear una categoría de aplicaciones con archivos ejecutables de dispositivos específicos

Puede usar archivos ejecutables almacenados en ciertos dispositivos puntuales como modelo de los archivos ejecutables que quiera permitir o bloquear. Los archivos ejecutables de estos dispositivos pueden servirle de base para crear una categoría, que luego podrá usar en la configuración del componente Control de aplicaciones.

*Para recuperar la lista de archivos ejecutables de los dispositivos:*

1. Asegúrese de que creó y activó una directiva para Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security para Windows. Habilite el componente Control de aplicaciones en la directiva.

2. Obtenga una lista de archivos ejecutables almacenados en los dispositivos cliente.

*Para crear una categoría que incluya archivos ejecutables de dispositivos seleccionados:*

1. En el menú principal, vaya a **Operaciones → Aplicaciones de terceros → Categorías de aplicaciones**.

   Se muestra una página con una lista de categorías.

2. Haga clic en el botón **Agregar**.

   Se inicia el Asistente para crear nueva categoría. Utilice el botón **Next** para avanzar a un nuevo paso del asistente.

3. En el paso **Seleccione un método para crear la categoría**, especifique el nombre para la categoría y seleccione la opción **Categoría que incluye los archivos ejecutables de los dispositivos seleccionados. Estos archivos ejecutables se procesan de forma automática y sus métricas se agregan a la categoría**.

4. Haga clic en **Agregar**.

5. En la ventana que se abre, seleccione el dispositivo que contenga los archivos ejecutables que desee usar para crear la categoría. Puede seleccionar más de un dispositivo.

6. Configure los siguientes ajustes:

- Algoritmo de evaluación del valor de hash

  Según la versión de la aplicación de seguridad instalada en los dispositivos en su red, debe seleccionar un algoritmo para que Kaspersky Security Center calcule el valor de hash para archivos en esta categoría. La información sobre los valores hash calculados por las funciones hash se almacena en la base de datos del Servidor de administración.

  SHA256 es una función de hash criptográfica. En la actualidad, se la considera la más confiable en su clase, pues no se encontró vulnerabilidad alguna en su algoritmo. Kaspersky Endpoint Security puede calcular hashes SHA256 desde la versión 10 Service Pack 2 para Windows. Las versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows son compatibles con la función de hash MD5.

  Seleccione cualquiera de las opciones de evaluación del valor de hash de Kaspersky Security Center para archivos en la categoría:

  - Si todas las instancias de aplicaciones de seguridad instaladas en su red son Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores, marque la casilla **SHA256**. Si hay versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows en su red, recomendamos que no agregue categorías que utilicen como criterio el hash SHA256 del archivo ejecutable. Si lo hace, la aplicación de seguridad podría no funcionar correctamente. De presentarse inconvenientes, utilice la función de hash criptográfico MD5 para los archivos de la categoría.

  - Si hay alguna versión anterior a Kaspersky Endpoint Security 10 Service Pack 2 para Windows instalada en su red, seleccione **Hash MD5**. No puede agregar una categoría que se haya creado según el criterio de la suma de verificación MD5 de un archivo ejecutable para Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores. De presentarse inconvenientes, utilice la función de hash criptográfico SHA256 para los archivos de la categoría.

  Si diferentes dispositivos en su red usan versiones anteriores y posteriores de Kaspersky Endpoint Security 10, marque la casilla **SHA256** y la casilla **Hash MD5**.

  La casilla **Calcular SHA256 para los archivos de esta categoría (compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)** está activada de manera predeterminada.

  De manera predeterminada, la casilla **Calcular MD5 para los archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)** está desactivada.

- Sincronizar datos con el repositorio del Servidor de administración

  Seleccione esta opción si desea que el Servidor de administración verifique periódicamente si ha habido cambios en la(s) carpeta(s) especificada(s).

  Esta opción está deshabilitada de forma predeterminada.

  Si habilita esta opción, indique la frecuencia (en horas) con la que se llevará a cabo la verificación. Por defecto, se realiza una búsqueda de cambios cada veinticuatro horas.

- Tipo de archivo

Utilice esta sección para especificar qué clase de archivos se usarán para crear la categoría de aplicaciones.

**Todos los archivos**. Para crear la categoría, se tendrán en cuenta todos los archivos. Esta opción está seleccionada de forma predeterminada.

**Solo archivos fuera de las categorías de aplicaciones**. Para crear la categoría, solo se tendrán en cuenta los archivos que no estén incluidos en las categorías de aplicaciones.

- **Carpetas**

  Utilice esta sección para elegir las carpetas del dispositivo (o de los dispositivos) que contengan los archivos que se usarán para crear la categoría de aplicaciones.

  **Todas las carpetas**. Para crear la categoría, se tendrán en cuenta todas las carpetas. Esta opción está seleccionada de forma predeterminada.

  **Carpeta especificada**: Para crear la categoría, solo se tendrá en cuenta la carpeta especificada. Si selecciona esta opción, deberá especificar la ruta a la carpeta.

Cuando finaliza el asistente, se crea la categoría para archivos ejecutables. se muestra en la lista de categorías. Podrá usar la categoría creada cuando configure Control de aplicaciones.

## Creación de una categoría de aplicaciones que incluya archivos ejecutables de una carpeta seleccionada

Puede usar archivos ejecutables de una carpeta seleccionada como el estándar de archivos ejecutables que desea permitir o bloquear en su organización. Sobre la base de los archivos ejecutables de la carpeta seleccionada, puede crear una categoría de aplicaciones y usarla en la configuración del componente Control de aplicaciones.

*Para crear una categoría que incluya archivos ejecutables de la carpeta seleccionada, haga lo siguiente:*

1. En el menú principal, vaya a **Operaciones** → **Aplicaciones de terceros** → **Categorías de aplicaciones**.

   Se muestra una página con una lista de categorías.

2. Haga clic en el botón **Agregar**.

   Se inicia el Asistente para crear nueva categoría. Utilice el botón **Next** para avanzar a un nuevo paso del asistente.

3. En el paso **Seleccione un método para crear la categoría**, especifique el nombre de la categoría y seleccione la opción **Categoría con los archivos ejecutables de una carpeta específica. Los archivos ejecutables de aplicaciones presentes en la carpeta especificada se procesan automáticamente y sus métricas se agregan a la categoría**.

4. Especifique la carpeta con los archivos ejecutables que se utilizarán para crear la categoría.

5. Defina los siguientes parámetros de configuración:

- **Incluir DLL en esta categoría**

  La categoría de aplicaciones incluye bibliotecas de enlace dinámico (archivos en el formato de DLL) y el componente Control de aplicaciones registra las acciones de esas bibliotecas que se ejecutan en el sistema. Incluir archivos DLL en la categoría podría reducir el rendimiento de Kaspersky Security Center.

  Esta casilla no está marcada de manera predeterminada.

- **Incluir datos de scripts en esta categoría**

  La categoría de aplicaciones incluye datos sobre scripts, y los scripts no son bloqueados por el componente Protección contra amenazas web. Incluir los datos del script en la categoría podría reducir el rendimiento de Kaspersky Security Center.

  Esta casilla no está marcada de manera predeterminada.

- **Algoritmo de evaluación del valor de hash**: **Calcular el hash SHA256 de los archivos de esta categoría (opción compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)/Calcular MD5 para los archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)**

Según la versión de la aplicación de seguridad instalada en los dispositivos en su red, debe seleccionar un algoritmo para que Kaspersky Security Center calcule el valor de hash para archivos en esta categoría. La información sobre los valores hash calculados por las funciones hash se almacena en la base de datos del Servidor de administración.

SHA256 es una función de hash criptográfica. En la actualidad, se la considera la más confiable en su clase, pues no se encontró vulnerabilidad alguna en su algoritmo. Kaspersky Endpoint Security puede calcular hashes SHA256 desde la versión 10 Service Pack 2 para Windows. Las versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows son compatibles con la función de hash MD5.

Seleccione cualquiera de las opciones de evaluación del valor de hash de Kaspersky Security Center para archivos en la categoría:

- Si todas las instancias de aplicaciones de seguridad instaladas en su red son Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores, marque la casilla **SHA256**. Si hay versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows en su red, recomendamos que no agregue categorías que utilicen como criterio el hash SHA256 del archivo ejecutable. Si lo hace, la aplicación de seguridad podría no funcionar correctamente. De presentarse inconvenientes, utilice la función de hash criptográfico MD5 para los archivos de la categoría.

- Si hay alguna versión anterior a Kaspersky Endpoint Security 10 Service Pack 2 para Windows instalada en su red, seleccione **Hash MD5**. No puede agregar una categoría que se haya creado según el criterio de la suma de verificación MD5 de un archivo ejecutable para Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores. De presentarse inconvenientes, utilice la función de hash criptográfico SHA256 para los archivos de la categoría.

Si diferentes dispositivos en su red usan versiones anteriores y posteriores de Kaspersky Endpoint Security 10, marque la casilla **SHA256** y la casilla **Hash MD5**.

La casilla **Calcular SHA256 para los archivos de esta categoría (compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)** está activada de manera predeterminada.

De manera predeterminada, la casilla **Calcular MD5 para los archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)** está desactivada.

- **Forzar análisis de cambios en carpeta**

Si se habilita esta opción, la aplicación buscará con frecuencia cambios en la carpeta de incorporación de contenido de categorías. Puede especificar la frecuencia de las búsquedas (en horas) en el campo de entrada que se encuentra al lado de la casilla de verificación. De forma predeterminada, el intervalo entre búsquedas forzadas es de 24 horas.

Si se deshabilita esta opción, la aplicación no forzará la búsqueda en la carpeta. El servidor intenta acceder a los archivos si se modificaron, agregaron o eliminaron.

Esta opción está deshabilitada de forma predeterminada.

Cuando finaliza el asistente, se crea la categoría de archivos ejecutables y se muestra en la lista de categorías. Puede usar la categoría en la configuración de Control de aplicaciones.

Para obtener información detallada sobre el Control de aplicaciones, consulte los siguientes temas de ayuda:

- Ayuda en línea de Kaspersky Endpoint Security para Windows
- Ayuda en línea de Kaspersky Endpoint Security for Linux

- Kaspersky Security for Virtualization Light Agent
- Ayuda de Kaspersky Embedded Systems Security para Windows
- Ayuda de Kaspersky Embedded Systems Security para Linux

## Visualización de la lista de categorías de aplicaciones

Puede ver la lista de las categorías configuradas de los archivos ejecutables y la configuración de cada una.

*Para ver la lista de categorías de aplicaciones:*

En el menú principal, vaya a **Operaciones** → **Aplicaciones de terceros** → **Categorías de aplicaciones**.

Se muestra una página con una lista de categorías.

*Para ver las propiedades de una categoría de aplicaciones:*

Haga clic en el nombre de la categoría.

Se muestra la ventana de propiedades de la categoría. Las propiedades se agrupan en varias pestañas.

## Agregar archivos ejecutables vinculados a eventos a una categoría de aplicaciones

Una vez que configure el componente Control de aplicaciones en las directivas de Kaspersky Endpoint Security para Windows, podrá ver los siguientes eventos en la lista de eventos:

- **Inicio de aplicación prohibido** (evento de nivel *Crítico*). Este evento se muestra si Control de aplicaciones se ha configurado para hacer cumplir sus reglas.
- **Inicio de aplicación prohibido en el modo de prueba** (evento de nivel *Información*). Este evento se muestra si Control de aplicaciones se ha configurado para aplicar sus reglas en modo de prueba.
- **Mensaje para el administrador sobre la prohibición de inicio de la aplicación** (*evento de Advertencia*). Este evento aparece si Control de aplicaciones se ha configurado para hacer cumplir sus reglas y un usuario ha solicitado acceso a una aplicación que no tiene permitido ejecutar.

Recomendamos crear selecciones de eventos para ver los eventos relacionados con el funcionamiento de Control de aplicaciones.

Puede agregar los archivos ejecutables vinculados a los eventos de Control de aplicaciones a una categoría de aplicaciones nueva o existente. En cualquiera de los dos casos, la categoría debe ser una categoría de aplicaciones con contenido agregado manualmente.

*Para agregar archivos ejecutables vinculados a los eventos de Control de aplicaciones a una categoría de aplicaciones:*

1. En el menú principal, vaya a **Supervisión e informes → Selecciones de eventos**.

   Se muestra la lista de selecciones de eventos.

2. Elija y genere una selección de eventos que le permita ver los eventos relacionados con Control de aplicaciones.

   Si no creó una selección de eventos relacionada con Control de aplicaciones, puede seleccionar y generar una de las selecciones predefinidas (por ejemplo, **Eventos recientes**).

   Se muestra la lista de eventos.

3. Seleccione los eventos asociados a los archivos ejecutables que desee agregar a la categoría de aplicaciones. A continuación, haga clic en el botón **Asignar a categoría**.

   Se inicia el Asistente para crear nueva categoría. Utilice el botón **Next** para avanzar a un nuevo paso del asistente.

4. En la página del asistente, configure los ajustes pertinentes:

- En la sección **Acción sobre archivo ejecutable relacionado con el evento**, seleccione una de las siguientes opciones:

  - **Agregar a una nueva categoría de aplicación**

    Seleccione esta opción si desea crear una nueva categoría de aplicaciones basada en los archivos ejecutables vinculados a los eventos.

    Esta opción está seleccionada de forma predeterminada.

    Si selecciona esta opción, escriba el nombre que tendrá la nueva categoría.

  - **Agregar a una categoría de aplicación existente**

    Seleccione esta opción si desea agregar los archivos ejecutables vinculados a los eventos a una categoría de aplicaciones existente.

    Esta opción no está seleccionada de manera predeterminada.

    Si selecciona esta opción, elija la categoría de aplicaciones con contenido agregado manualmente a la que desee agregar los archivos ejecutables.

- En la sección **Tipo de reglas**, seleccione una de las siguientes opciones:

  - **Reglas para agregar a inclusiones**
  - **Reglas para agregar a exclusiones**

- En la sección **Parámetro utilizado como condición**, seleccione una de las siguientes opciones:

  - **Detalles del certificado (o hashes SHA256 para archivos sin certificado)**

    Los archivos pueden estar firmados con un certificado. Cada certificado puede utilizarse para firmar más de un archivo. Un mismo certificado puede usarse para firmar distintas versiones de una misma aplicación, por ejemplo, o distintas aplicaciones de un mismo proveedor. Cuando seleccione un certificado, podría suceder que la categoría termine con varias versiones de una misma aplicación o con varias aplicaciones de un mismo proveedor.

    Cada archivo tiene su propia función hash SHA256. Si selecciona una función hash SHA256, solo se agregará a la categoría el archivo específico que se corresponda con ese hash (por ejemplo, la versión especificada de la aplicación).

    Seleccione esta opción si desea agregar los detalles del certificado de un archivo ejecutable (o la función hash SHA256 de los archivos sin certificado) a las reglas de la categoría.

    Esta opción está seleccionada de forma predeterminada.

  - **Detalles del certificado (los archivos sin certificado se omitirán)**

Los archivos pueden estar firmados con un certificado. Cada certificado puede utilizarse para firmar más de un archivo. Un mismo certificado puede usarse para firmar distintas versiones de una misma aplicación, por ejemplo, o distintas aplicaciones de un mismo proveedor. Cuando seleccione un certificado, podría suceder que la categoría termine con varias versiones de una misma aplicación o con varias aplicaciones de un mismo proveedor.

Seleccione esta opción si desea agregar los detalles del certificado de un archivo ejecutable a las reglas de la categoría. Si el archivo ejecutable no tiene certificado, el archivo se omitirá. No se agregará información sobre ese archivo a la categoría.

- **Solo SHA256 (los archivos sin hash se omitirán)**

  Cada archivo tiene su propia función hash SHA256. Si selecciona una función hash SHA256, solo se añadirá a la categoría el archivo específico que se corresponda con ese hash (por ejemplo, la versión especificada de la aplicación).

  Seleccione esta opción si solo desea agregar los detalles de la función hash SHA256 del archivo ejecutable.

- **Solo MD5 (modo discontinuado, solo para Kaspersky Endpoint Security 10 Service Pack 1)**

  Cada archivo tiene su propia función hash MD5. Si selecciona una función hash MD5, solo se agregará a la categoría el archivo específico que se corresponda con ese hash (por ejemplo, la versión especificada de la aplicación).

  Seleccione esta opción si solo desea agregar los detalles de la función hash MD5 del archivo ejecutable. La capacidad de calcular hashes MD5 está disponible para Kaspersky Endpoint Security 10 Service Pack 1 para Windows y versiones anteriores.

5. Haga clic en **Aceptar**.

   Cuando finaliza el asistente, los archivos ejecutables vinculados a los eventos de Control de aplicaciones se agregan a la categoría de aplicaciones nueva o existente. Puede ver la configuración de la categoría de aplicaciones creada o modificada.

Para obtener información detallada sobre el Control de aplicaciones, consulte los siguientes temas de ayuda:

- Ayuda en línea de Kaspersky Endpoint Security para Windows
- Ayuda en línea de Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Ayuda de Kaspersky Embedded Systems Security para Windows
- Ayuda de Kaspersky Embedded Systems Security para Linux

## Configurar Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows

Tras crear las categorías de Control de aplicaciones, puede utilizarlas para configurar el componente en las directivas de Kaspersky Endpoint Security para Windows.

*Para configurar Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.

   Se muestra una página con una lista de directivas.

2. Haga clic en la directiva de **Kaspersky Endpoint Security para Windows**.

   Se abre la ventana de configuración de la directiva.

3. Vaya a **Configuración de la aplicación** → **Controles de seguridad** → **Control de aplicaciones**.

   Se abre la ventana **Control de aplicaciones**, en la que encontrará los ajustes de Control de aplicaciones.

4. La opción **Control de aplicaciones** está habilitada de manera predeterminada. Asegúrese de que el botón de alternancia **Control de aplicaciones DESACTIVADO** se encuentre en la posición desactivada.

5. En el bloque de opciones **Configuración de Control de aplicaciones**, habilite el modo de funcionamiento pertinente para aplicar las reglas de Control de aplicaciones y permitir que Kaspersky Endpoint Security para Windows bloquee el inicio de aplicaciones.

   Si desea probar las reglas de Control de aplicaciones, en la sección **Configuración de Control de aplicaciones**, habilite el modo de prueba. Cuando el modo de prueba está habilitado, Kaspersky Endpoint Security para Windows no bloquea el inicio de las aplicaciones, pero registra información sobre las reglas activadas en el informe. Haga clic en el vínculo **Ver informe** para ver esa información.

6. Habilite la opción **Controlar la carga de módulos DLL** si desea que Kaspersky Endpoint Security para Windows monitoree la carga de módulos DLL cuando los usuarios inicien aplicaciones.

   Se guardará un informe con datos sobre los módulos y sobre las aplicaciones que carguen esos módulos.

   Kaspersky Endpoint Security para Windows únicamente atenderá a los módulos DLL y controladores que se carguen después de que habilite la opción **Controlar la carga de módulos DLL**. Reinicie el dispositivo después de habilitar la opción **Controlar la carga de módulos DLL** si desea que Kaspersky Endpoint Security para Windows supervise la carga de todos los módulos DLL y controladores, incluidos aquellos que se carguen antes de la ejecución de Kaspersky Endpoint Security para Windows.

7. (Opcional). En el bloque **Plantillas de mensajes**, modifique la plantilla del mensaje que se le muestra al usuario cuando se le impide iniciar una aplicación y la plantilla del correo electrónico que el usuario le puede enviar a usted.

8. En el bloque de opciones **Modo de Control de aplicaciones**, seleccione el modo **Lista de rechazados** o el modo **Lista de admitidos**.

   De forma predeterminada, está seleccionado el modo **Lista de rechazados**.

9. Haga clic en el vínculo **Configuración de las listas de reglas**.

   Se abre la ventana **Listas de rechazados y admitidos** que permite agregar una categoría de aplicaciones. De manera predeterminada, la pestaña **Lista de rechazados** está seleccionada si se selecciona el modo **Lista de rechazados**, o la pestaña **Lista de admitidos** si se selecciona el modo **Lista de admitidos**.

10. En la ventana **Listas de rechazados y admitidos**, haga clic en el botón **Agregar**.

    Se abre la ventana **Regla de Control de aplicaciones**.

11. Haga clic en el vínculo **Debe elegir una categoría**.

    Se abre la ventana **Categoría de aplicaciones**.

12. Agregue la categoría de aplicaciones (o las categorías de aplicaciones) que creó anteriormente.

    Si desea modificar la configuración de una categoría que creó, haga clic en el botón **Editar**.

    Si desea crear una nueva categoría, haga clic en el botón **Agregar**.

    Si desea eliminar una categoría de la lista, haga clic en el botón **Eliminar**.

13. Una vez que la lista de categorías de aplicaciones esté completa, haga clic en el botón **Aceptar**.

    Se cierra la ventana **Categoría de aplicaciones**.

14. En la ventana de la regla de **Control de aplicaciones**, en la sección **Usuarios y sus derechos**, cree una lista con los usuarios y grupos de usuarios a los que se aplicará la regla de Control de aplicaciones.

15. Haga clic en el botón **Aceptar** para guardar la configuración y cerrar la ventana **Regla de Control de aplicaciones**.

16. Haga clic en el botón **Aceptar** para guardar la configuración y cerrar la ventana **Listas de rechazados y admitidos**.

17. Haga clic en el botón **Aceptar** para guardar la configuración y cerrar la ventana **Control de aplicaciones**.

18. Cierre la ventana con la configuración de la directiva de Kaspersky Endpoint Security para Windows.

    Se guarda la configuración de Control de aplicaciones. Una vez que la directiva se propague a los dispositivos cliente, el inicio de archivos ejecutables estará bajo su control.

Para obtener información detallada sobre el Control de aplicaciones, consulte los siguientes temas de ayuda:

- Ayuda en línea de Kaspersky Endpoint Security para Windows
- Ayuda en línea de Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Ayuda de Kaspersky Embedded Systems Security para Windows
- Ayuda de Kaspersky Embedded Systems Security para Linux

## Obtener y ver una lista de aplicaciones instaladas en los dispositivos cliente

Kaspersky Security Center hace un inventario de todo el software instalado en los dispositivos cliente administrados que ejecutan Linux y Windows.

El Agente de red elabora una lista de las aplicaciones instaladas en un dispositivo y luego transmite la lista al Servidor de administración. El Agente de red tarda entre 10 y 15 minutos en actualizar la lista de aplicaciones.

Para los dispositivos cliente basados en Windows, el Agente de red recibe la mayor parte de la información sobre las aplicaciones instaladas del registro de Windows. Para los dispositivos cliente basados en Linux, los administradores de paquetes brindan información al Agente de red sobre las aplicaciones instaladas.

Si se detectó una aplicación en la sección **Registro de aplicaciones** en un dispositivo Linux, las propiedades de la aplicación no contienen información sobre los archivos ejecutables relacionados.

*Para ver la lista de las aplicaciones instaladas en los dispositivos administrados:*

1. En el menú principal, vaya a **Operaciones** → **Aplicaciones de terceros** → **Registro de aplicaciones**.

   La página muestra una tabla con las aplicaciones que están instaladas en los dispositivos administrados. Seleccione la aplicación para ver sus propiedades, por ejemplo, el nombre del proveedor, número de versión, lista de archivos ejecutables, lista de dispositivos en los que está instalada la aplicación, lista de actualizaciones de software disponibles o la lista de vulnerabilidades de software detectadas.

2. Puede agrupar y filtrar los datos de la tabla con las aplicaciones instaladas de la siguiente manera:

   - Haga clic en el icono de configuración ( ) en la esquina superior derecha de la tabla.

     En el menú invocado **Configuración de las columnas**, seleccione las columnas que se mostrarán en la tabla. Para ver el tipo de sistema operativo de los dispositivos cliente en los que está instalada la aplicación, seleccione la columna **Tipo de sistema operativo**.

   - Haga clic en el icono de filtro ( ) en la esquina superior derecha de la tabla y luego especifique y aplique el criterio de filtro en el menú invocado.

     Se muestra la tabla filtrada de aplicaciones instaladas.

*Para visualizar la lista de aplicaciones instaladas en un dispositivo administrado en particular, haga lo siguiente:*

En el menú principal, vaya a **Dispositivos** → **Dispositivos administrados** → **<device name>** → **Avanzado** → **Registro de aplicaciones**. En este menú, puede exportar la lista de aplicaciones a un archivo CSV o TXT.

Para obtener información detallada sobre el Control de aplicaciones, consulte los siguientes temas de ayuda:

- Ayuda en línea de Kaspersky Endpoint Security para Windows
- Ayuda en línea de Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Ayuda de Kaspersky Embedded Systems Security para Windows
- Ayuda de Kaspersky Embedded Systems Security para Linux

# Crear un paquete de instalación para una aplicación de terceros usando la base de datos de Kaspersky

Kaspersky Security Center Web Console le permite realizar la instalación remota de aplicaciones de terceros mediante el uso de paquetes de instalación. Las aplicaciones de terceros se incluyen en una base de datos dedicada de Kaspersky. Esta base de datos se crea automáticamente cuando se ejecuta la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* por primera vez.

*Para crear un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky, haga lo siguiente:*

1. En el menú principal, vaya a **Descubrimiento y despliegue** → **Despliegue y asignación** → **Paquetes de instalación**.

2. Haga clic en el botón **Agregar**.

3. En la página Asistente de nuevo paquete que se abre, seleccione la opción **Seleccionar una aplicación de la base de datos de Kaspersky para crear un paquete de instalación** y luego haga clic en **Siguiente**.

4. En la lista de aplicaciones que se abre, seleccione la aplicación correspondiente y luego haga clic en **Siguiente**.

5. Seleccione el idioma de localización relevante en la lista desplegable y luego haga clic en **Siguiente**.

   Este paso solo se muestra si la aplicación brinda varias opciones de idioma.

6. Si se le solicita que acepte un Acuerdo de licencia para la instalación, en la página **Contrato de licencia de usuario final** que se abre, haga clic en el vínculo para leer el Contrato de licencia en el sitio web del proveedor y luego seleccione la casilla de verificación **Confirmo que he leído completamente, entiendo y acepto los términos y las condiciones de este Contrato de licencia de usuario final**.

7. En la página **Nombre del nuevo paquete de instalación** que se abre, en el campo **Nombre del paquete**, ingrese el nombre del paquete de instalación y luego haga clic en **Siguiente**.

Espere hasta que el paquete de instalación recién creado se cargue en el Servidor de administración. Cuando el Asistente de nuevo paquete muestre el mensaje que le informa que el proceso de creación del paquete se realizó correctamente, haga clic en **Finalizar**.

El paquete de instalación recién creado aparecerá en la lista de paquetes de instalación. Puede seleccionar este paquete al crear o reconfigurar la tarea *Instalar aplicación de forma remota*.

# Ver y modificar la configuración de un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky

Si creó un paquete de instalación para algunas de las aplicaciones de terceros incluidas en la base de datos de Kaspersky, puede ver y modificar posteriormente la configuración de esto paquete.

La modificación de la configuración de un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky solo está disponible con la licencia Administración de vulnerabilidades y parches.

Para ver y modificar la configuración de un paquete de instalación de una aplicación de terceros incluida en la base de datos de Kaspersky:

1. En el menú principal, vaya a **Descubrimiento y despliegue → Despliegue y asignación → Paquetes de instalación**.

2. En la lista de paquetes de instalación que se abre, haga clic en el nombre del paquete pertinente.

3. En la página de propiedades que se abre, modifique la configuración, si es necesario.

4. Haga clic en el botón **Guardar**.

Se guarda la configuración modificada.

# Configurar el paquete de instalación de una aplicación de terceros incluida en la base de datos de Kaspersky

La configuración de un paquete de instalación de una aplicación de terceros se agrupa en las siguientes pestañas:

Solo una parte de la configuración que se muestra a continuación se muestra de forma predeterminada, por lo que puede agregar las columnas correspondientes haciendo clic en **Filtrar** y seleccionando los nombres de columna relevantes de la lista.

- Pestaña **General**:
  - Campo de entrada que contiene el nombre del paquete de instalación que se puede editar manualmente
  - Aplicación

    El nombre de la aplicación de terceros para la que se creó el paquete de instalación.
  - Versión

    El número de versión de la aplicación de terceros para la que se creó el paquete de instalación.
  - Tamaño

    El tamaño del paquete de instalación de terceros (en kilobytes).
  - Creado

    La fecha y la hora en que se creó el paquete de instalación de terceros.
  - Ruta

    La ruta a la carpeta de red donde se almacena el paquete de instalación de terceros.
- Pestaña **Procedimiento de instalación**:
  - Instalar los componentes generales obligatorios del sistema

    Si esta opción está habilitada, antes de que se instale una actualización, la aplicación instalará automáticamente todos los componentes generales del sistema que la actualización requiera para instalarse (los llamados "requisitos previos"). Una actualización podría requerir, por ejemplo, que esté instalada cierta actualización del sistema operativo.

    Si esta opción está deshabilitada, posiblemente tenga que instalar los requisitos previos manualmente.

    Esta opción está deshabilitada de forma predeterminada.
  - Tabla que muestra las propiedades de actualización y que contiene las siguientes columnas:

- **Nombre**

  Nombre de la actualización.

- **Descripción**

  Descripción de la actualización.

- **Origen**

  El origen de la actualización, es decir, si fue publicada por Microsoft o por un desarrollador externo diferente.

- **Tipo**

  El tipo de actualización, es decir, si la actualización está destinada a un controlador o una aplicación.

- **Categoría**

  La categoría de Windows Server Update Services (WSUS) que se muestra para las actualizaciones de Microsoft (Actualizaciones críticas, Actualizaciones de las definiciones, Controladores, Paquetes de características, Actualizaciones de seguridad, Service Packs, Herramientas, Paquetes acumulativos de actualizaciones, Actualizaciones o Upgrade).

- **Nivel de importancia conforme a MSRC**

  El nivel de importancia de la actualización definido por el Centro de respuesta de seguridad de Microsoft (MSRC).

- **Nivel de importancia**

  El nivel de importancia de la actualización definido por Kaspersky.

- **Nivel de importancia del parche**

  El nivel de importancia del parche si está destinado a una aplicación de Kaspersky.

- **Artículo**

  El identificador (id.) del artículo de la Base de conocimientos que describe la actualización.

- **Boletín**

  El id. del boletín de seguridad que describe la actualización.

- **Instalación no asignada (nueva versión)**

  Muestra si la actualización tiene el estado Instalación no asignada.

- **Por instalarse**

  Muestra si la actualización tiene el estado Por instalarse.

- **Instalándose**

  Muestra si la actualización tiene el estado Instalándose.

- **Instalada**

  Muestra si la actualización tiene el estado Instalada.

- **Error**

  Muestra si la actualización tiene el estado Error.

- **Se debe reiniciar el dispositivo**

  Muestra si la actualización tiene el estado Se debe reiniciar el dispositivo.

- **Registrada**

  Muestra la fecha y hora en que se registró la actualización.

- **Instalada en modo interactivo**

  Muestra si la actualización solicita la intervención del usuario durante la instalación.

- **Revocado**

  Muestra la fecha y hora en que se revocó la actualización.

- **Estado de aprobación de la actualización**

  Muestra si la instalación de la actualización está aprobada.

- **Revisión**

  Muestra el número de revisión actual de la actualización.

- **Id. de actualización**

  Muestra el id. de la actualización.

- **Versión de la aplicación**

  Muestra el número de versión a la que se actualizará la aplicación.

- **Reemplazada**

  Muestra otras actualizaciones que pueden reemplazar a la actualización.

- **Reemplaza**

  Muestra otras actualizaciones que pueden ser reemplazadas por la actualización.

- **Debe aceptar los términos del Contrato de licencia**

  Muestra si la actualización solicita aceptar los términos de un contrato de licencia de usuario final (EULA).

- **Dirección URL de descripción**

  Muestra el nombre del proveedor de la actualización.

- **Familia de aplicaciones**

  Muestra el nombre de la familia de aplicaciones a las que pertenece la actualización.

- **Aplicación**

  Muestra el nombre de la aplicación a la que pertenece la actualización.

- **Idioma de localización**

  Muestra el idioma de localización de la actualización.

- **Instalación no asignada (nueva versión)**

  Muestra si la actualización tiene el estado Instalación no asignada (nueva versión).

- **Requiere instalación de requisitos previos**

  Muestra si la actualización tiene el estado Requiere instalación de requisitos previos.

- **Modo de descarga**

  Muestra el modo de descarga de la actualización.

- **Es un parche**

  Muestra si la actualización es un parche.

- **Sin instalar**

  Muestra si la actualización tiene el estado Sin instalar.

- Pestaña **Configuración** que muestra la configuración del paquete de instalación (con sus nombres, descripciones y valores) que se utilizan como parámetros de la línea de comandos durante la instalación. Si el paquete no proporciona dicha configuración, se muestra el mensaje correspondiente. Puede modificar los valores de esta configuración.

- Pestaña **Historial de revisiones** que muestra las revisiones del paquete de instalación y que contiene las siguientes columnas:

  - **Revisión**: muestra el número de revisión de los paquetes de instalación.

  - **Hora**: fecha y hora en que se modificó la configuración del paquete de instalación.

  - **Usuario**: nombre del usuario que modificó la configuración del paquete de instalación.

  - **Acción**: acción realizada sobre el paquete de instalación dentro de la revisión.

  - **Descripción**: descripción de la revisión vinculada al cambio realizado en la configuración del paquete de instalación.

    De manera predeterminada, la descripción de las revisiones está en blanco. Para agregar una descripción a una revisión, seleccione la revisión pertinente y haga clic en el botón **Editar descripción**. En la ventana abierta, ingrese un texto que describa la revisión.

# Etiquetas de aplicación

Kaspersky Security Center le permite etiquetar las aplicaciones desde el registro de aplicaciones. Las etiquetas son rótulos que se asignan a las aplicaciones y que pueden utilizarse para agruparlas o encontrarlas. Asignada a una serie de aplicaciones, una etiqueta puede servir de condición para crear una selección de dispositivos.

Por ejemplo, puede crear la etiqueta `[Navegadores]` y asignarla a todos los navegadores, como Microsoft Internet Explorer, Google Chrome y Mozilla Firefox.

## Creación de una etiqueta de aplicación

*Para crear una etiqueta de aplicación:*

1. En el menú principal, vaya a **Operaciones** → **Aplicaciones de terceros** → **Etiquetas de aplicación**.

2. Haga clic en **Agregar**.

   Se abre una ventana para crear la etiqueta.

3. Introduzca el nombre de la etiqueta.

4. Haga clic en **Aceptar** para guardar los cambios.

La nueva etiqueta aparece en la lista de etiquetas de aplicación.

## Cambiar el nombre de una etiqueta de aplicación

*Para cambiar el nombre de una etiqueta de aplicación:*

1. En el menú principal, vaya a **Operaciones → Aplicaciones de terceros → Etiquetas de aplicación**.
2. Marque la casilla ubicada junto a la etiqueta a la que desee cambiarle el nombre y haga clic en **Editar**.

   Se abre la ventana de propiedades de la etiqueta.
3. Cambie el nombre de la etiqueta.
4. Haga clic en **Aceptar** para guardar los cambios.

La etiqueta actualizada aparece en la lista de etiquetas de aplicación.

## Asignación de etiquetas a una aplicación

*Para asignar una o varias etiquetas a una aplicación:*

1. En el menú principal, vaya a **Operaciones → Aplicaciones de terceros → Registro de aplicaciones**.
2. Haga clic en el nombre de la aplicación a la que desee asignar las etiquetas.
3. Seleccione la pestaña **Etiquetas**.

   En la pestaña, verá todas las etiquetas de aplicación que existan en el Servidor de administración. Las etiquetas que estén asignadas a la aplicación elegida tendrán una casilla activada en la columna **Modo de asignación**.
4. Busque las etiquetas que desee asignar y active las casillas de verificación correspondientes en la columna **Modo de asignación**.
5. Haga clic en **Guardar** para guardar los cambios.

Se asignan las etiquetas a la aplicación.

## Quitarle una etiqueta a una aplicación

*Para quitarle una o más etiquetas a una aplicación:*

1. En el menú principal, vaya a **Operaciones → Aplicaciones de terceros → Registro de aplicaciones**.
2. Haga clic en el nombre de la aplicación a la que desee quitarle etiquetas.
3. Seleccione la pestaña **Etiquetas**.

   En la pestaña, verá todas las etiquetas de aplicación que existan en el Servidor de administración. Las etiquetas que estén asignadas a la aplicación elegida tendrán una casilla activada en la columna **Modo de asignación**.

4. Busque las etiquetas que desee quitarle a la aplicación y desactive las casillas de verificación correspondientes en la columna **Modo de asignación**.

5. Haga clic en **Guardar** para guardar los cambios.

Se le quitan las etiquetas seleccionadas a la aplicación.

Las etiquetas de aplicación desasignadas no se eliminan. Si lo desea, puede eliminarlas manualmente.

## Eliminación de una etiqueta de aplicación

*Para eliminar una etiqueta de aplicación:*

1. En el menú principal, vaya a **Operaciones** → **Aplicaciones de terceros** → **Etiquetas de aplicación**.

2. En la lista, seleccione la etiqueta de aplicación que desee eliminar.

3. Haga clic en el botón **Eliminar**.

4. En la ventana que se abre, haga clic en **Aceptar**.

Se elimina la etiqueta de aplicación. La etiqueta eliminada se borra automáticamente de las aplicaciones a las que estaba asignada.

# Supervisión e informes

Esta sección describe las capacidades de supervisión e informes de Kaspersky Security Center. Estas prestaciones permiten obtener una visión general de la infraestructura, ver los estados de protección y acceder a información estadística.

Después del despliegue de Kaspersky Security Center o durante la operación, puede configurar las funciones de supervisión e informes para que se adapten mejor a sus necesidades.

# Procedimiento: Supervisión y generación de informes

En esta sección se describe un escenario para configurar la característica de supervisión y generación de informes de Kaspersky Security Center.

### Requisitos previos

Cuando Kaspersky Security Center se haya implementado en la red de su organización, podrá supervisar su funcionamiento y generar informes al respecto.

El proceso de supervisar la red de una organización y generar informes se divide en etapas:

1. **Configurar cambios de estado para los dispositivos**

   Familiarícese con los ajustes que permiten cambiar el estado de los dispositivos en respuesta a distintas condiciones. Al cambiar estas configuraciones, puede cambiar la cantidad de eventos con niveles de importancia *Crítica* o *Advertencia*. Cuando configure los cambios de estados para los dispositivos, preste especial atención a lo siguiente:

   - La nueva configuración no debe contravenir las políticas de seguridad de datos de su organización.
   - Puede reaccionar a eventos de seguridad importantes en la red de su organización de manera oportuna.

2. **Configurar las notificaciones sobre los eventos que suceden en los dispositivos cliente**

   Instrucciones:

   Configure la notificación (por correo electrónico, SMS o ejecutando un archivo ejecutable) de eventos en dispositivos cliente

3. **Cambiar el modo en que la red de seguridad responde al evento Brote de virus**

   Puede modificar los umbrales específicos en las propiedades del Servidor de administración. También puede crear una directiva más estricta que se activará o crear una tarea que se ejecutará cuando ocurra este evento.

4. **Realización de acciones recomendadas para notificaciones críticas, de advertencia e informativas**

   Instrucciones:

   Realizar acciones recomendadas para la red de su organización

5. **Controlar el estado de seguridad de la red de la organización**

   Instrucciones:

   - Revisión del widget Estado de protección
   - Generación y revisión del Informe del estado de la protección
   - Genere y revise el Informe de errores

6. **Buscar dispositivos cliente que no se encuentren protegidos**

   Instrucciones:

   - Revise el widget Nuevos dispositivos
   - Genere y revise el Informe del despliegue de la protección

7. **Controlar la protección de los dispositivos cliente**

   Instrucciones:

   - Generación y revisión de informes de las categorías Estado de protección y Estadísticas de amenazas
   - Inicie y revise la selección de eventos Crítico

8. **Evaluar y limitar el impacto de los eventos en la base de datos**

   Se transfiere la información sobre eventos que ocurren durante el funcionamiento de aplicaciones administradas de un dispositivo cliente y se registra en la base de datos del Servidor de administración. Para reducir la carga del Servidor de administración, evalúe y limite la cantidad de eventos que se guardan como máximo en la base de datos.

   Instrucciones:

- Evaluación de espacio de la base de datos
- Limitar el número máximo de eventos

9. **Controlar la información de las licencias**

   Instrucciones:

   - Añadir el widget Uso de clave de licencia al panel y revisarlo
   - Genere y revise el Informe de uso de claves de licencia

### Resultados

Al concluir este escenario, podrá mantenerse al corriente de la protección de su red y estará en condiciones de planificar medidas de protección adicionales.

## Acerca de los tipos de funciones de supervisión y generación de informes

La información sobre eventos de seguridad en la red de una organización se almacena en la base de datos del Servidor de administración. En función de los eventos, Kaspersky Security Center Web Console proporciona los siguientes tipos de monitoreo e informes en la red de su organización:

- Panel
- Informes
- Selecciones de eventos
- Notificaciones

### Panel

El panel brinda información gráfica que ayuda a controlar las tendencias de seguridad que se presentan en la red de la organización.

### Informes

La función Informes permite obtener información numérica detallada sobre la seguridad de la red de la organización. La información puede guardarse en un archivo, imprimirse o enviarse por correo electrónico.

### Selecciones de eventos

Las selecciones de eventos brindan una vista en pantalla de distintos conjuntos de eventos, que se toman de la base de datos del Servidor de administración y se identifican con un nombre. Estos conjuntos de eventos se agrupan y clasifican de distintas maneras:

- Por nivel de importancia: **Eventos críticos**, **Errores funcionales**, **Advertencias** y **Eventos informativos**

- Por fecha: **Eventos recientes**
- Por tipo: **Solicitudes de usuario** y **Eventos de auditoría**

Puede usar los ajustes disponibles en la interfaz de Kaspersky Security Center Web Console para ver y crear selecciones de eventos definidas por el usuario.

### Notificaciones

Las notificaciones le alertan acerca de eventos y le ayudan a acelerar sus respuestas a estos eventos mediante la realización de acciones recomendadas o acciones que considere apropiadas.

# Panel y widgets

En esta sección, se brinda información sobre el panel y sobre los widgets que el panel ofrece. Aquí encontrará instrucciones para administrar los widgets y configurar los ajustes de los widgets.

## Uso del panel

El panel brinda información gráfica que ayuda a controlar las tendencias de seguridad que se presentan en la red de la organización.

Para acceder al panel en Kaspersky Security Center Web Console, haga clic en **Panel** en la sección **Supervisión e informes**.

El panel ofrece widgets personalizables. Existe una gran selección de widgets diferentes, presentados en forma de tablas, listas y gráficos de barras, líneas y anillos. La información que se muestra en los widgets se actualiza automáticamente; el período de actualización es de uno a dos minutos. El intervalo entre actualizaciones varía de un widget a otro. Puede actualizar los datos de un widget manualmente en cualquier momento a través del menú de configuración.

De forma predeterminada, los widgets incluyen información sobre todos los eventos almacenados en la base de datos del Servidor de administración.

Kaspersky Security Center Web Console tiene un conjunto predeterminado de widgets de las siguientes categorías:

- **Estado de protección**
- **Despliegue**
- **Actualización**
- **Estadísticas de amenazas**
- **Otros**

Algunos widgets tienen información de texto con vínculos. Puede hacer clic en esos vínculos para acceder a información detallada.

Al configurar el panel, puede agregar los widgets que le resulten necesarios, ocultar los widgets que no precise, cambiar el tamaño o el aspecto de los widgets, mover los widgets y cambiar la configuración de los widgets.

## Agregar widgets al panel

*Para agregar widgets al panel:*

1. En el menú principal, vaya a **Supervisión e informes** → **Panel**.
2. Haga clic en el botón **Agregar o restaurar widget web**.
3. En la lista de widgets disponibles, seleccione los widgets que desee agregar al panel.

   Los widgets se agrupan por categoría. Para ver los widgets que forman parte de una categoría, haga clic en el corchete angular (>) ubicado junto al nombre de la categoría en cuestión.
4. Haga clic en el botón **Agregar**.

Los widgets seleccionados se agregan al final del panel.

Si lo desea, puede modificar el aspecto y la configuración de los widgets agregados.

## Ocultar un widget del panel

*Para ocultar uno de los widgets que se muestran en el panel:*

1. En el menú principal, vaya a **Supervisión e informes** → **Panel**.
2. Haga clic en el ícono de configuración (⚙) ubicado junto al widget que desee ocultar.
3. Seleccione **Ocultar widget web**.
4. En la ventana **Advertencia** que se abre, haga clic en **Aceptar**.

Se oculta el widget seleccionado. Más tarde, podrá agregar el widget al panel nuevamente.

## Mover un widget en el panel

*Para mover un widget en el panel:*

1. En el menú principal, vaya a **Supervisión e informes** → **Panel**.
2. Haga clic en el ícono de configuración (⚙) ubicado junto al widget que desee mover.
3. Seleccione **Mover**.
4. Haga clic en la ubicación a la que desee mover el widget. Solo puede seleccionar una ubicación que se encuentre ocupada por otro widget.

Los widgets cambiarán de ubicación recíprocamente.

## Cambiar el aspecto o el tamaño de un widget

Puede modificar el aspecto de los widgets que contienen un gráfico y hacer que muestren un gráfico de barras o un gráfico de líneas. Algunos widgets también están disponibles en distintos tamaños (compacto, medio y máximo) y pueden redimensionarse.

*Para cambiar el aspecto de un widget:*

1. En el menú principal, vaya a **Supervisión e informes** → **Panel**.
2. Haga clic en el ícono de configuración (⚙) ubicado junto al widget que desee modificar.
3. Realice una de las siguientes acciones:
   - Para que el widget se muestre como gráfico de barras, seleccione **Tipo de gráfico: barras**.
   - Para que el widget se muestre como gráfico de líneas, seleccione **Tipo de gráfico: líneas**.
   - Para cambiar el área ocupada por el widget, seleccione uno de los siguientes valores:
     - **Compacto**
     - **Compacto (solo barra)**
     - **Medio (gráfico de anillos)**
     - **Medio (diagrama de barras)**
     - **Máximo**

El widget seleccionado toma el nuevo aspecto.

## Cambiar la configuración de un widget

*Para modificar la configuración de un widget:*

1. En el menú principal, vaya a **Supervisión e informes** → **Panel**.
2. Haga clic en el ícono de configuración (⚙) ubicado junto al widget que desee cambiar.
3. Seleccione **Mostrar configuración**.
4. En la ventana de configuración del widget, haga los cambios que desee en los ajustes del widget.
5. Haga clic en **Guardar** para guardar los cambios.

Se modifican los ajustes del widget seleccionado.

El conjunto de ajustes disponibles varía según el widget. Estos son algunos de los ajustes comunes:

- **Alcance del widget web** (conjunto de objetos de los que muestra la información el widget): por ejemplo, un grupo de administración o selección de dispositivos.
- **Elija una tarea**: tarea a la que corresponde la información mostrada por el widget.
- **Intervalo de tiempo** (el intervalo de tiempo durante el cual se muestra la información en el widget): entre las dos fechas especificadas; desde la fecha especificada hasta el día actual; o desde el día actual menos el número especificado de días hasta el día actual.
- **Fijar en Crítico si esto se cumple** y **Fijar en Advertencia si esto se cumple**: las reglas que determinan el color de un semáforo.

Después de cambiar la configuración del widget, puede actualizar los datos en el widget manualmente.

*Para actualizar datos en un widget:*

1. En el menú principal, vaya a **Supervisión e informes** → **Panel**.
2. Haga clic en el ícono de configuración (⚙) ubicado junto al widget que desee mover.
3. Seleccione **Actualizar**.

Se actualizan los datos del widget.

## Acerca del modo solo panel

Puede configurar el modo solo panel para aquellos empleados que, sin ser responsables por la administración de la red, desean ver información estadística sobre la protección de la red en Kaspersky Security Center. Esta información podría resultar de interés para un alto ejecutivo, por ejemplo. Un usuario para el que se habilitado el modo solo panel tiene acceso únicamente a un panel con un conjunto de widgets predefinido. La persona puede monitorear las estadísticas que brinda cada widget (por ejemplo, el estado de protección de los dispositivos administrados, la cantidad de amenazas detectadas en tiempo reciente o la lista de amenazas más frecuentes en la red).

Un usuario para el que se habilitado el modo solo panel está sujeto a las siguientes restricciones:

- El usuario no tiene acceso al menú principal, lo cual le impide modificar los ajustes de protección de la red.
- El usuario no puede realizar ninguna acción con los widgets: no puede, por ejemplo, agregar widgets nuevos ni quitar los widgets agregados. Debido a estas restricciones, usted deberá agregar al panel todos los widgets que el usuario precise y deberá encargarse, asimismo, de configurarlos (tendrá que fijar la regla de conteo de objetos, definir el intervalo de tiempo, etc.).

Un usuario no puede asignarse a sí mismo el modo solo panel. Si desea trabajar en este modo, comuníquese con su administrador de sistemas, con su proveedor de servicios administrados (MSP) o con un usuario que tenga el derecho **Modificar ACL de objetos** en el área funcional **Características generales: Permisos de usuario**.

# Configuración del modo solo panel

Si desea configurar el modo solo panel, asegúrese primero de que se cumplan los siguientes requisitos:

- Usted cuenta con el derecho **Modificar ACL de objetos** en el área funcional **Características generales: Permisos de usuario**. Si no tiene este derecho, no encontrará la pestaña para configurar el modo.
- El usuario tiene asignado el derecho Leer en el área funcional **Características generales**: **Funcionalidad básica**.

Si creó una jerarquía de Servidores de administración en su red, para configurar el modo solo panel, vaya al Servidor que tenga disponible la cuenta de usuario en la pestaña **Usuarios** de la sección **Usuarios y roles** → **Usuarios y grupos**. El servidor puede ser un servidor principal o un servidor secundario físico. Este modo no puede ajustarse en servidores virtuales.

*Para configurar el modo solo panel:*

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
2. Haga clic en el nombre de la cuenta de usuario para la que desee ajustar el panel con widgets.
3. En la ventana que se abre, que contendrá los ajustes de la cuenta, seleccione la pestaña **Panel**.

   En la pestaña que se abre, verá un panel. El panel será el mismo panel para usted que para el usuario.
4. Si la opción **Mostrar la consola en modo solo panel** está habilitada, cambie la posición del interruptor para deshabilitarla.

   El sistema no le permitirá hacer cambios en el panel mientras esta opción se encuentre habilitada. Una vez que deshabilite esta opción, podrá operar con los widgets.
5. Configure la apariencia del panel. El conjunto de widgets preparados en la pestaña **Panel** estará disponible para el usuario con la cuenta personalizable. El usuario no podrá agregar widgets nuevos al panel ni podrá quitar los widgets agregados; tampoco podrá modificar los ajustes o el tamaño de estos elementos. Debido a estas limitaciones, debe ocuparse usted de ajustar los widgets de manera tal que el usuario tenga acceso a las estadísticas sobre la protección de la red. A tal fin, la pestaña **Panel** le permitirá operar con los widgets tal como si estuviera en la sección **Supervisión e informes** → **Panel**. Podrá hacer lo siguiente:
   - Agregar nuevos widgets al panel.
   - Ocultar widgets que el usuario no necesite.
   - Mover los widgets y colocarlos en otro orden.
   - Cambiar el tamaño o el aspecto de los widgets.
   - Modificar los ajustes de los widgets.
6. Active el interruptor para habilitar la opción **Mostrar la consola en modo solo panel**.

   Una vez que habilite esta opción, el usuario solamente tendrá acceso al panel. Podrá ver las estadísticas, pero no podrá hacer cambios en los ajustes de protección de la red ni podrá modificar el aspecto del panel. Como el panel es el mismo para usted que para el usuario, usted tampoco podrá hacer ajustes en el panel.

   Si deja esta opción deshabilitada, el usuario tendrá acceso al menú principal y, desde allí, podrá realizar distintas acciones en Kaspersky Security Center, como modificar los widgets y cambiar los ajustes de seguridad.

7. Haga clic en el botón **Guardar** cuando haya terminado de configurar el modo solo panel. El usuario no verá el panel preparado sino hasta que usted guarde los cambios.

8. Si el usuario desea ver las estadísticas de las aplicaciones de Kaspersky compatibles y necesita, para ello, contar con determinados derechos de acceso, configure los derechos del usuario. Tras ello, el usuario verá los datos de las aplicaciones de Kaspersky en los widgets correspondientes a esas aplicaciones.

Al concluir este procedimiento, el usuario podrá iniciar sesión en Kaspersky Security Center con su cuenta personalizada y utilizar el modo solo panel para monitorear las estadísticas sobre la protección de la red.

# Informes

En esta sección, se brindan instrucciones para trabajar con los informes, administrar plantillas de informes personalizadas, usar plantillas de informes para generar nuevos informes y crear tareas de entrega de informes.

## Utilización de informes

La función Informes permite obtener información numérica detallada sobre la seguridad de la red de la organización. La información puede guardarse en un archivo, imprimirse o enviarse por correo electrónico.

Para acceder a los informes en Kaspersky Security Center Web Console, ingrese a la sección **Supervisión e informes** y haga clic en **Informes**.

Por defecto, los informes contienen información de los últimos treinta días.

Kaspersky Security Center tiene un conjunto predeterminado de informes de las siguientes categorías:

- **Estado de protección**
- **Despliegue**
- **Actualización**
- **Estadísticas de amenazas**
- **Otros**

Puede crear plantillas de informe personalizadas y modificar o eliminar las plantillas de informe existentes.

Puede crear informes basados en las plantillas existentes, exportar informes a archivos y crear tareas de entrega de informes.

## Crear una plantilla de informe

*Para crear una plantilla de informe:*

1. En el menú principal, vaya a **Supervisión e informes** → **Informes**.
2. Haga clic en **Agregar**.

   Se abre el Asistente de nueva plantilla de informe. Avance por el asistente utilizando el botón **Siguiente**.
3. Ingrese el nombre del informe y seleccione el tipo de informe.
4. En el paso **Alcance** del asistente, seleccione el conjunto de dispositivos cliente (grupo de administración, selección de dispositivos, dispositivos seleccionados o todos los dispositivos de red) cuyos datos se mostrarán en informes que se basen en esta plantilla de informe.
5. En el paso **Período del informe**, especifique el período del informe. Los valores disponibles son los siguientes:

   - Entre dos fechas específicas
   - Desde una fecha específica hasta la fecha de creación del informe
   - Desde cierta cantidad de días antes de la creación del informe hasta la fecha de creación del informe

   Esta página puede no aparecer para algunos informes.
6. Haga clic en **Aceptar** para cerrar el asistente.
7. Realice una de las siguientes acciones:

   - Haga clic en el botón **Guardar y ejecutar** para guardar la nueva plantilla de informe y crear un informe basado en ella.

     Se guardará la plantilla de informe. Se generará el informe.
   - Haga clic en el botón **Guardar** para guardar la nueva plantilla de informe.

     Se guardará la plantilla de informe.

Puede utilizar la nueva plantilla para generar y ver informes.

## Ver y editar las propiedades de una plantilla de informe

Puede ver y editar las propiedades básicas de las plantillas de informe (por ejemplo, el nombre de las plantillas o los campos que se muestran en los informes).

*Para ver y editar las propiedades de una plantilla de informe:*

1. En el menú principal, vaya a **Supervisión e informes** → **Informes**.
2. Marque la casilla ubicada junto a la plantilla de informe cuyas propiedades desee ver o editar.

   Como alternativa, genere un informe y luego haga clic en el botón **Editar**.

3. Haga clic en el botón **Abrir las propiedades de la plantilla del informe**.

   Se abre la ventana **Editando informe "<nombre del informe>"**. La pestaña **General** estará seleccionada.

4. Modifique las propiedades de la plantilla de informe:

- Pestaña **General**:
  - Nombre de la plantilla de informe
  - Cantidad máxima de entradas para mostrar

    Si esta opción está habilitada, la tabla con los datos detallados del informe mostrará, como máximo, el número de entradas indicado aquí.

    Las entradas del informe se ordenan primero siguiendo las reglas especificadas en la sección **Campos** → **Campos Detalles** de las propiedades de la plantilla de informe, y luego se conservan solo las primeras de las entradas resultantes. El encabezado de la tabla con los datos detallados del informe indica el número de entradas mostradas y el total de entradas disponibles que coinciden con otros parámetros de la plantilla del informe.

    Si deshabilita esta opción, se mostrarán todas las entradas disponibles en la tabla con los datos detallados del informe. No recomendamos deshabilitar esta opción. Al limitar el número de entradas que se muestran en un informe, se aminora la carga en el sistema de administración de bases de datos y se reduce el tiempo requerido para generar y exportar el informe. Algunos de los informes contienen demasiadas entradas. En tales casos, no es sencillo leer y analizar todas las entradas. Además, cuando se genera un informe de este tipo, se corre el riesgo de que el dispositivo se quede sin memoria; de ocurrir este problema, no será posible siquiera ver el informe.

    Esta opción está activada de forma predeterminada. El valor predeterminado es 1000.

  - **Grupo**

    Haga clic en el botón **Configuración** para cambiar el conjunto de dispositivos cliente para los que se crea el informe. Este botón puede no estar disponible para algunos tipos de informes. La configuración aplicada depende de la configuración especificada durante la creación de la plantilla de informe.

  - **Intervalo de tiempo**

    Haga clic en el botón **Configuración** para modificar el período comprendido por el informe. Este botón puede no estar disponible para algunos tipos de informes. Los valores disponibles son los siguientes:

    - Entre dos fechas específicas
    - Desde una fecha específica hasta la fecha de creación del informe
    - Desde cierta cantidad de días antes de la creación del informe hasta la fecha de creación del informe

  - Incluir datos de los Servidores de administración secundarios y virtuales

    Cuando esta opción se encuentra habilitada, el informe incluye información de los servidores de administración secundarios y virtuales que están subordinados al Servidor de administración para el cual se ha creado la plantilla de informe.

    Deshabilite esta opción si solo desea ver datos del Servidor de administración con el que está trabajando.

    Esta opción está activada de forma predeterminada.

  - Hasta el nivel de anidamiento

El informe incluirá datos de los servidores de administración secundarios y virtuales que se encuentren <n> o más niveles de anidamiento por debajo del Servidor de administración con el que se esté trabajando, siendo <n> el valor especificado.

El valor predeterminado es 1. Puede cambiar este valor si necesita recuperar información de servidores de administración secundarios que se encuentren aún más abajo en el árbol.

- Intervalo de espera de datos (min)

  Antes de generar el informe, el Servidor de administración para el que se haya creado la plantilla de informe esperará, durante el tiempo especificado, a que los servidores de administración secundarios le envíen datos. Transcurrido este período de espera, el Servidor generará el informe aunque no haya recibido información de los servidores de administración secundarios. En ese caso, en lugar de los datos reales, el informe mostrará el valor **N/D** (no disponible) o, si la opción **Almacenar en caché los datos de los Servidores de administración secundarios** está habilitada, mostrará información tomada de la caché.

  El valor predeterminado es 5 (minutos).

- Almacenar en caché los datos de los Servidores de administración secundarios

  Los servidores de administración secundarios transfieren datos periódicamente al Servidor de administración para el que se ha creado la plantilla de informe. Una vez allí, los datos transferidos se guardan en una caché.

  Si, al momento de generar un informe, el Servidor de administración no puede recibir datos de algún Servidor de administración secundario, el informe contendrá los datos de esta caché. La fecha en que los datos se transfirieron a la caché estará indicada en el informe.

  Si habilita esta opción, podrá ver datos de los servidores de administración secundarios incluso cuando no se pueda obtener información actualizada. Sin embargo, los datos mostrados podrían ser obsoletos.

  Esta opción está deshabilitada de forma predeterminada.

- Frecuencia de actualización de la caché (h)

  Los servidores de administración secundarios transfieren datos a intervalos regulares al Servidor de administración para el que se ha creado la plantilla de informe. Puede especificar el largo de este intervalo en horas. Si fija el valor en 0 horas, solamente se transferirá información cuando se genere el informe.

  El valor predeterminado es 0.

- Transferir información detallada desde los Servidores de administración secundarios

En el informe generado, la tabla con los datos detallados del informe contendrá datos de los servidores de administración secundarios que estén subordinados al Servidor de administración para el cual se haya creado la plantilla de informe.

Si habilita esta opción, los informes tardarán más tiempo en generarse y habrá más tráfico entre los servidores de administración. Sin embargo, podrá ver toda la información en un solo informe.

En lugar de habilitar esta opción, podría analizar los datos detallados de un informe para detectar un Servidor de administración secundario con problemas y, hecho esto, generar ese mismo informe únicamente para ese Servidor de administración.

Esta opción está deshabilitada de forma predeterminada.

- Pestaña **Campos**

  Seleccione los campos que se mostrarán en el informe y ordénelos con los botones **Subir** y **Bajar**. Use los botones **Agregar** o **Editar** para especificar si los campos se usarán para filtrar y ordenar los datos del informe.

  La sección **Filtros de los campos Detalles** contiene un botón llamado **Convertir filtros**. Haga clic en este botón para comenzar a usar el formato de filtrado ampliado. Este formato permite combinar, mediante la operación lógica OR, las condiciones de filtrado especificadas en distintos campos. Si hace clic en el botón, se abrirá el panel **Convertir filtros** en el lado derecho. Haga clic en el botón **Convertir filtros** para confirmar la conversión. Tras ello, podrá definir un filtro convertido con condiciones de la sección **Campos Detalles** que se apliquen utilizando la operación lógica OR.

  Cuando un informe se convierte al formato que permite definir condiciones de filtrado complejas, el mismo deja de ser compatible con las versiones anteriores de Kaspersky Security Center (11 y anteriores). Los informes convertidos no incluyen datos de servidores de administración secundarios basados en versiones incompatibles.

5. Haga clic en **Guardar** para guardar los cambios.
6. Cierra la ventana **Editando informe "<nombre del informe>"**.

La plantilla de informe actualizada aparece en la lista de plantillas de informe.

## Exportación de un informe a un archivo

Puede exportar un informe a un archivo XML, HTML o PDF.

*Para exportar un informe a un archivo:*

1. En el menú principal, vaya a **Supervisión e informes** → **Informes**.
2. Marque la casilla ubicada junto al informe que desee exportar a un archivo.
3. Haga clic en el botón **Exportar informe**.
4. En la ventana que se abre, cambiar el nombre del archivo del informe a través del campo **Nombre**. De forma predeterminada, el nombre del archivo coincide con el nombre de la plantilla de informe seleccionada.

5. Seleccione el tipo de archivo al que se exportará el informe: XML, HTML o PDF.

6. Haga clic en el botón **Exportar informe**.

   El informe se descargará en el formato seleccionado. El archivo se guardará en la carpeta predeterminada del dispositivo o se abrirá la ventana **Guardar como** estándar del navegador para que pueda guardarlo donde desee.

El informe se guarda en el archivo.

## Generar y ver un informe

*Para crear y ver un informe:*

1. En el menú principal, vaya a **Supervisión e informes** → **Informes**.

2. Haga clic en el nombre de la plantilla de informe con la que desee crear el informe.

Se creará y mostrará un informe basado en la plantilla seleccionada.

Los datos del informe se muestran respetando los ajustes de localización definidos para el Servidor de administración.

El informe contendrá los siguientes datos:

- En la pestaña **Resumen**:
  - El nombre del informe, el tipo de informe, una descripción breve, el período comprendido por el informe e información sobre el grupo de dispositivos para los que se generó el informe.
  - Un gráfico con los datos más representativos del informe.
  - Una tabla unificada con los indicadores calculados del informe.
- En la pestaña **Detalles**, una tabla con datos detallados del informe.

## Crear una tarea de entrega de informes

Puede crear una tarea para entregar informes específicos.

*Para crear una tarea de entrega de informes:*

1. En el menú principal, vaya a **Supervisión e informes** → **Informes**.

2. Active las casillas ubicadas junto a las plantillas de informe para las que desee crear una tarea de entrega de informes.

3. Haga clic en el botón **Crear tarea de entrega**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

4. En el paso **Configuración de tarea nueva** del asistente, ingrese el nombre de la tarea.

   El nombre predeterminado es **Entregar informes**. Si ya existe una tarea con este nombre, se agrega un número de secuencia (<N>) al nombre de la tarea.

5. En el paso **Configuración del informe** del asistente, especifique la siguiente configuración:

   a. Seleccione las plantillas de informe que entregará la tarea.

   b. Defina el formato de los informes: HTML, XLS o PDF.

      Se requiere la herramienta wkhtmltopdf para convertir un informe a PDF. Cuando selecciona la opción PDF, el Servidor de administración verifica si la herramienta wkhtmltopdf está instalada en el dispositivo. Si la herramienta no está instalada, la aplicación muestra un mensaje sobre la necesidad de instalar la herramienta en el dispositivo del Servidor de administración. Instale la herramienta manualmente y luego continúe con el siguiente paso.

   c. Indique si los informes se enviarán por correo electrónico y, de ser así, defina los ajustes de notificación por correo electrónico.

      Puede especificar hasta 20 direcciones de correo electrónico. Para separar direcciones de correo electrónico, presione **Intro**. También puede pegar una lista de direcciones de correo electrónico separadas por comas y luego presionar **Intro**.

   d. Si los informes se guardarán en una carpeta, si los informes guardados anteriormente en esta carpeta se sobrescribirán y si una cuenta específica se usará para acceder a la carpeta (para una carpeta compartida).

6. En el paso **Configurar programación de tarea** del asistente, seleccione la programación de inicio de la tarea.

   Están disponibles las siguientes opciones de programación de tareas:

- **Manual**

  La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

  Esta opción está seleccionada de forma predeterminada.

- **Cada N minutos**

  La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

  De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

- **Cada N horas**

  La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

  De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

- **Cada N días**

  La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

  De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

- **Cada N semanas**

  La tarea se ejecutará periódicamente, a intervalos regulares, en el día de la semana y a la hora que especifique. Cada ejecución estará separada de la anterior por el número de semanas que indique.

  Por defecto, la tarea se ejecutará cada lunes a la hora actual del sistema.

- **Mensual**

  La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

  Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

  Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

- **En los días especificados**

La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

Por defecto, la hora de inicio es a las 18:00 y no se selecciona ningún día del mes.

Tenga en cuenta que no selecciona una fecha específica en el mes, ni el número de la semana (primera, segunda semana del mes), sino el número de secuencia del día de la semana dentro de un mes. Por ejemplo, si coloca el cursor en la celda **Ma** de la **Primero** fila, significa que la tarea se ejecutará el primer martes de cada mes nuevo.

Puede seleccionar varios días de la semana.

- **Ante brotes de virus**

  La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para defensa del perímetro
  - Antivirus para sistemas de correo

  Por defecto, están seleccionados todos los tipos de aplicaciones.

  En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- **Al completarse otra tarea**

  La tarea actual se iniciará después de que se complete otra tarea. Esta opción solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

7. En este paso del asistente, configure otras opciones de programación de tareas:

- En la sección **Programación de la tarea**, verifique o reconfigure la programación previamente seleccionada, y establezca el intervalo de tiempo, los días del mes o la semana, establezca la condición de brote de virus o la finalización de otra tarea como disparador para iniciar la tarea. También se puede especificar una hora de inicio en esta sección si se selecciona una programación aplicable.

- En la sección **Configuración adicional**, especifique las siguientes configuraciones:

  - **Ejecutar tareas no realizadas**

    Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

    Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

    Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

    Esta opción está deshabilitada de forma predeterminada.

  - **Utilizar retardo aleatorio automático para el inicio de la tarea**

    Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

    La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

    Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

  - **Utilizar el retardo aleatorio automático para el inicio de la tarea dentro de un intervalo de**

    Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

    Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

    Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

  - **Detener la tarea si tarda más de**

Una vez que transcurra el período especificado, la tarea se detendrá automáticamente, se haya completado o no.

Habilite esta opción si desea que las tareas que tarden mucho en completarse se interrumpan o se detengan.

Esta opción está deshabilitada de forma predeterminada. El tiempo de ejecución por defecto para las tareas es de 120 minutos.

8. En el paso **Seleccione una cuenta con la que ejecutar la tarea** del asistente, especifique las credenciales de la cuenta de usuario que se utiliza para ejecutar la tarea.

9. Si desea modificar otras configuraciones de la tarea después de crearla, en el paso **Finalizar la creación de la tarea** del asistente, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** (esta opción está habilitada de manera predeterminada).

10. Haga clic en el botón **Finalizar** para crear la tarea y cerrar el asistente.

    Se creará la tarea de entrega de informes. Si la opción **Abrir los detalles de la tarea cuando se complete la creación** está habilitada, se abrirá la ventana de configuración de la tarea.

## Eliminación de plantillas de informes

*Para eliminar una o varias plantillas de informes:*

1. En el menú principal, vaya a **Supervisión e informes** → **Informes**.

2. Marque las casillas ubicadas junto a las plantillas de informes que desee eliminar.

3. Haga clic en el botón **Eliminar**.

4. En la ventana que se abre, haga clic en **Aceptar** para confirmar su selección.

Se eliminan las plantillas de informes seleccionadas. Si las plantillas formaban parte de una o más tareas de entrega de informes, se las eliminará también de esas tareas.

# Eventos y selecciones de eventos

En esta sección, se brinda información sobre los eventos y las selecciones de eventos, sobre los tipos de eventos que ocurren en los componentes de Kaspersky Security Center y sobre cómo puede administrar el bloqueo de eventos frecuentes.

## Acerca de los eventos de Kaspersky Security Center

Kaspersky Security Center le permite recibir información sobre los eventos de funcionamiento del Servidor de administración y aplicaciones de Kaspersky instaladas en dispositivos administrados. La información sobre estos eventos se guarda en la base de datos del Servidor de administración.

## Tipos de evento

En Kaspersky Security Center existen los siguientes tipos de eventos:

- Eventos generales. Esta clase de evento ocurre en todas las aplicaciones de Kaspersky administradas. Un ejemplo de evento general es Brote de virus. Los eventos generales tienen una sintaxis y una semántica estrictamente definidas. Los eventos generales se utilizan en, por ejemplo, los paneles e informes.
- Eventos específicos de las aplicaciones de Kaspersky administradas. Cada aplicación de Kaspersky administrada tiene su propio conjunto de eventos.

## Orígenes de eventos

Los eventos pueden ser generados por las siguientes aplicaciones:

- Componentes de Kaspersky Security Center:
  - Servidor de administración
  - Agente de red
  - Servidor de MDM para iOS
  - Servidor de dispositivos móviles Exchange
- Aplicaciones administradas por Kaspersky

  Para obtener detalles sobre los eventos generados por las aplicaciones administradas por Kaspersky, consulte la documentación de la aplicación correspondiente.

Puede ver la lista completa de los eventos que puede generar una aplicación en la pestaña **Configuración de eventos** en la directiva de la aplicación. Para el Servidor de administración, también puede ver la lista de eventos en las propiedades del Servidor de administración.

## Nivel de importancia de los eventos

Cada evento tiene su propio nivel de importancia. El nivel de importancia que se le asigna a un evento puede variar según las circunstancias en las que ocurre. Existen cuatro niveles de importancia:

- Un *evento crítico* es un evento que se registra cuando ocurre un problema de extrema gravedad, que puede derivar en pérdidas de información, en un error crítico o en un fallo de funcionamiento.
- Un *error funcional* es un evento que se registra cuando ocurre un problema, fallo o error graves en el funcionamiento de la aplicación o en la ejecución de un procedimiento.
- Una *advertencia* es un evento que no necesariamente es grave, pero que anticipa un posible problema en el futuro. La mayoría de los eventos se catalogan como advertencias si, a pesar de que el evento haya ocurrido, la aplicación puede recuperarse sin sufrir una pérdida de información o de funcionalidad.
- Un evento *informativo* es un evento que se registra para informar que una operación o procedimiento se completaron sin errores o que la aplicación funciona correctamente.

Cada evento tiene un plazo de almacenamiento definido, durante el cual lo puede ver o modificar en Kaspersky Security Center. Algunos eventos no se guardan en la base de datos del Servidor de administración de forma predeterminada porque su plazo de almacenamiento está definido en cero. Para que un evento pueda exportarse, debe permanecer almacenado al menos un día en la base de datos del Servidor de administración.

## Utilización de selecciones de eventos

Las selecciones de eventos brindan una vista en pantalla de distintos conjuntos de eventos, que se toman de la base de datos del Servidor de administración y se identifican con un nombre. Estos conjuntos de eventos se agrupan y clasifican de distintas maneras:

- Por nivel de importancia: **Eventos críticos**, **Errores funcionales**, **Advertencias** y **Eventos informativos**
- Por fecha: **Eventos recientes**
- Por tipo: **Solicitudes de usuario** y **Eventos de auditoría**

Puede usar los ajustes disponibles en la interfaz de Kaspersky Security Center Web Console para ver y crear selecciones de eventos definidas por el usuario.

Para acceder a las selecciones de eventos disponibles en Kaspersky Security Center Web Console, vaya a la sección **Supervisión e informes** y haga clic en **Selecciones de eventos**.

De manera predeterminada, las selecciones de eventos incluyen información de los últimos siete días.

Kaspersky Security Center tiene un conjunto predeterminado de las selecciones (predefinidas) del evento:

- Eventos con distintos niveles de importancia:
  - **Eventos críticos**
  - **Errores funcionales**
  - **Advertencias**
  - **Eventos informativos**
- **Solicitudes de usuario** (eventos de aplicaciones administradas)
- **Eventos recientes** (de la semana anterior)
- Eventos de auditoría.

De ser necesario, puede crear y configurar selecciones adicionales, llamadas selecciones definidas por el usuario. Los eventos de estas selecciones pueden filtrarse de distintas maneras: utilizando las propiedades de los dispositivos que dieron origen a los eventos (el nombre, el intervalo IP y el grupo de administración de esos dispositivos), por tipo de evento, por nivel de gravedad del evento, por intervalo de tiempo y por nombre de aplicación y componente. El ámbito de búsqueda también puede incluir resultados de tareas. Existe además un campo de búsqueda simple, que permite escribir una o varias palabras. Utilice este campo para que se muestren todos los eventos que contengan, en cualquiera de sus atributos (nombre del evento, descripción, nombre del componente, etc.), alguna de las palabras indicadas.

Puede limitar el número de eventos que se muestran y el número de registros que se buscan tanto en las selecciones predefinidas como en las selecciones definidas por el usuario. Ambas opciones afectan al tiempo que tarda Kaspersky Security Center en mostrar los eventos. Cuanto más grande es la base de datos, más lento puede ser el proceso.

Puede hacer lo siguiente:

- Editar propiedades de selecciones de eventos
- Generar selecciones de eventos
- Ver detalles de las selecciones de eventos
- Eliminar selecciones de eventos
- Eliminar eventos de la base de datos del Servidor de administración

## Crear una selección de eventos

*Para crear una selección de eventos:*

1. En el menú principal, vaya a **Supervisión e informes** → **Selecciones de eventos**.
2. Haga clic en **Agregar**.
3. En la ventana **Nueva selección de eventos** que se abre, defina los ajustes de la nueva selección de eventos. Haga esto en una o varias de las secciones de la ventana.
4. Haga clic en **Guardar** para guardar los cambios.

   Se abre la ventana de confirmación.
5. Para ver el resultado de la selección de eventos, deje marcada la casilla **Ir al resultado de la selección**.
6. Haga clic en **Guardar** para confirmar que desea crear la selección de eventos.

Si dejó marcada la casilla **Ir al resultado de la selección**, verá el resultado de la selección de eventos. De lo contrario, encontrará la nueva selección de eventos en la lista de selecciones de eventos.

## Editar una selección de eventos

*Para editar una selección de eventos:*

1. En el menú principal, vaya a **Supervisión e informes** → **Selecciones de eventos**.
2. Marque la casilla ubicada junto a la selección de eventos que desee editar.
3. Haga clic en el botón **Propiedades**.

   Se abrirá una ventana para configurar la selección de eventos.

4. Modifique las propiedades de la selección de eventos.

> Si eligió una selección de eventos predefinida, solo podrá editar las propiedades disponibles en las pestañas **General** (excepto el nombre de la selección), **Hora** y **Derechos de acceso**.

Si eligió una selección de eventos definida por el usuario, podrá editar cualquiera de las propiedades.

5. Haga clic en **Guardar** para guardar los cambios.

La selección de eventos editada se muestra en la lista.

## Ver una lista de una selección de eventos

*Para ver una selección de eventos:*

1. En el menú principal, vaya a **Supervisión e informes** → **Selecciones de eventos**.
2. Marque la casilla ubicada junto a la selección de eventos que desee iniciar.
3. Realice una de las siguientes acciones:
   - Si desea configurar la clasificación en el resultado de la selección de eventos, haga lo siguiente:
     a. Haga clic en el botón **Reconfigurar la clasificación e iniciar**.
     b. Cuando se abra la ventana **Reconfigurar la clasificación para la selección de eventos**, ajuste las opciones de clasificación.
     c. Haga clic en el nombre de la selección.
   - Si, por el contrario, desea ver la lista de eventos tal como están ordenados en el Servidor de administración, haga clic en el nombre de la selección.

Se muestra el resultado de la selección de eventos.

## Exportar una selección de eventos

Kaspersky Security Center permite guardar una selección de eventos y su configuración en un archivo KLO. El archivo KLO puede usarse para importar la selección de eventos guardada en Kaspersky Security Center Windows o Kaspersky Security Center Linux.

> Tenga en cuenta que solo puede exportar selecciones de eventos definidas por el usuario. Las selecciones de eventos del conjunto predeterminado de Kaspersky Security Center (selecciones predefinidas) no se pueden guardar en un archivo.

*Para exportar una selección de eventos:*

1. En el menú principal, vaya a **Supervisión e informes → Selecciones de eventos**.
2. Marque la casilla ubicada junto a la selección de eventos que desee exportar.

   No es posible exportar más de una selección de eventos a la vez. Si selecciona más de una selección, el botón **Exportar** se desactivará.
3. Haga clic en el botón **Exportar**.
4. En la ventana abierta **Guardar como**, especifique el nombre y la ruta del archivo de selección de eventos y luego haga clic en el botón **Guardar**.

   La ventana **Guardar como** aparecerá solo si utiliza los navegadores Google Chrome, Microsoft Edge u Opera. Si utiliza otro navegador, el archivo de la selección de eventos se guardará automáticamente en la carpeta **Descargas**.

## Importar una selección de eventos

Kaspersky Security Center Cloud permite importar una selección de eventos de un archivo KLO. El archivo KLO contiene la selección de eventos exportada y su configuración.

*Para importar una selección de eventos:*

1. En el menú principal, vaya a **Supervisión e informes → Selecciones de eventos**.
2. Haga clic en el botón **Importar** y luego elija un archivo de selección de eventos que desee importar.
3. En la ventana que se abre, especifique la ruta al archivo KLO y haga clic en el botón **Abrir**. Tenga en cuenta que no podrá seleccionar más de un archivo de selección de eventos.

   Comienza el procesamiento de selección de eventos.

Aparecerá una notificación con los resultados de la importación. Si la selección de eventos se importa correctamente, puede hacer clic en el vínculo **Ver detalles de importación** para ver las propiedades de la selección de eventos.

Una vez que se complete la importación, la selección de eventos aparece en la lista de selección. Los ajustes de la selección de eventos también se importan.

Si la selección de eventos importada tiene el mismo nombre que una selección de eventos existente, el nombre de la selección importada se complementa con un índice secuencial en formato **(<siguiente número secuencial>)**, por ejemplo **(1)**, **(2)**.

## Ver los detalles de un evento

*Para ver los detalles de un evento:*

1. Genere una selección de eventos.
2. Haga clic en la hora del evento por el que desee consultar.
   Se abre la ventana **Propiedades del evento**.
3. En la ventana que se abre, puede hacer lo siguiente:
   - Ver la información del evento seleccionado
   - Ir a los eventos que se encuentran antes y después del elegido en el resultado de la selección de eventos
   - Ir al dispositivo en el que ocurrió el evento
   - Ir al grupo de administración del dispositivo en el que ocurrió el evento
   - Si el evento está relacionado con una tarea, ir a las propiedades de esa tarea

## Exportar eventos a un archivo

Kaspersky Security Center le permite guardar eventos de una selección de eventos en un archivo TXT.

*Para exportar eventos a un archivo:*

1. Genere una selección de eventos.
2. Marque la casilla ubicada junto al evento pertinente.
   También puede seleccionar varios eventos o la selección de eventos completa.
3. Haga clic en el botón **Exportar a archivo**.

El evento seleccionado se exporta a un archivo TXT.

## Acceder al historial de un objeto desde un evento

Puede acceder al historial de revisiones de un objeto compatible con la administración de revisiones desde un evento relacionado con la creación o modificación de ese objeto.

*Para acceder al historial de un objeto desde un evento:*

1. Genere una selección de eventos.
2. Marque la casilla ubicada junto al evento pertinente.
3. Haga clic en el botón **Historial de revisiones**.

   Se abre el historial de revisiones del objeto.

## Eliminar eventos

*Para eliminar uno o varios eventos:*

1. Genere una selección de eventos.
2. Active las casillas de verificación ubicadas junto a los eventos pertinentes.
3. Haga clic en el botón **Eliminar**.

   Los eventos seleccionados se eliminan. No los podrá recuperar.

## Eliminación de selecciones de eventos

Solo es posible eliminar selecciones de eventos definidas por el usuario. Las selecciones de eventos predefinidas no se pueden eliminar.

*Para eliminar una o varias selecciones de eventos:*

1. En el menú principal, vaya a **Supervisión e informes → Selecciones de eventos**.
2. Marque las casillas ubicadas junto a las selecciones de eventos que desee eliminar.
3. Haga clic en **Eliminar**.
4. En la ventana que se abre, haga clic en **Aceptar**.

   Se elimina la selección de eventos.

## Configuración del plazo de almacenamiento para un evento

Kaspersky Security Center le permite recibir información sobre los eventos de funcionamiento del Servidor de administración y aplicaciones de Kaspersky instaladas en dispositivos administrados. La información sobre estos eventos se guarda en la base de datos del Servidor de administración. Puede que deba almacenar algunos eventos durante un periodo más largo o más corto que el que se especifica en los valores predeterminados. Puede cambiar la configuración predeterminada del término de almacenamiento para un evento.

Si no le interesa almacenar algunos eventos en la base de datos del Servidor de administración, puede deshabilitar la configuración adecuada en la directiva del Servidor de administración y la directiva de la aplicación de Kaspersky, o en las propiedades del Servidor de administración (solo para eventos del Servidor de administración). Esto reducirá el número de tipos de evento en la base de datos.

Cuanto más largo sea el término de almacenamiento para un evento, más rápidamente alcanzará su capacidad máxima la base de datos. Al mismo tiempo, cuanto mayor sea el plazo de almacenamiento, más extenso será el período que podrán abarcar las tareas de supervisión y generación de informes.

*Para establecer el término de almacenamiento para un evento en la base de datos del Servidor de administración:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en el nombre de la directiva pertinente.

   Puede seleccionar una directiva de una aplicación de Kaspersky administrada, un Agente de red o un Servidor de administración. Para el Servidor de administración, también puede configurar el plazo de almacenamiento de los eventos haciendo clic en el ícono de configuración ( ) junto al nombre del Servidor de administración requerido.

3. Seleccione la pestaña **Configuración de eventos**.

   Se muestra una lista de los tipos de evento relacionados con la sección **Crítico**. Si es necesario, puede pasar a la sección **Error funcional**, **Advertencia** o **Información**.

4. En la lista de tipos de evento en el panel derecho, haga clic en el vínculo del evento cuyo término de almacenamiento desea cambiar.

   En la sección **Registro de los eventos** de la ventana que se abre, la opción **Guardar en la base de datos del Servidor de administración por (días)** está habilitada.

5. En el cuadro de edición debajo de este botón de alternancia, introduzca la cantidad de días para almacenar el evento.

6. Si no desea almacenar un evento en la base de datos del Servidor de administración, deshabilite la opción **Guardar en la base de datos del Servidor de administración por (días)**.

   Si configura los eventos del Servidor de administración en la ventana de propiedades del Servidor de administración, y si la configuración del evento está bloqueada en la directiva del Servidor de administración de Kaspersky Security Center, no podrá redefinir el valor del plazo de almacenamiento para un evento.

7. Haga clic en **Aceptar** y, una vez que se cierre el panel derecho, haga clic en el botón **Guardar**.

   La ventana de propiedades de la directiva está cerrada.

En lo sucesivo, cuando el Servidor de administración reciba y almacene los eventos del tipo seleccionado, se aplicará el plazo de almacenamiento modificado. El Servidor de administración no cambiará el plazo de almacenamiento de los eventos ya recibidos.

## Eventos de los componentes de Kaspersky Security Center

Cada componente de Kaspersky Security Center tiene su propio conjunto de tipos de evento. En esta sección, se enumeran los tipos de eventos que ocurren en el Servidor de administración de Kaspersky Security Center, el Agente de red y el Servidor de MDM para iOS. Los tipos de eventos que pueden ocurrir en las aplicaciones de Kaspersky no se detallan en esta sección.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Para el Servidor de administración, también puede ver y configurar la lista de eventos en las propiedades del Servidor de administración. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

## Estructura de datos utilizada para describir los tipos de eventos

Cada tipo de evento tiene especificado su nombre, identificador (id.), código alfabético, descripción y plazo de almacenamiento predeterminado.

- **Nombre que se muestra para el tipo de evento**. Este texto se muestra en Kaspersky Security Center cuando configura los eventos y cuando ocurren.
- **Id. del tipo de evento**. Un código numérico que se utiliza para procesar los eventos con una herramienta de análisis de eventos desarrollada por un tercero.
- **Tipo de evento** (código alfabético). Este código se usa cuando navega y procesa eventos utilizando vistas públicas que se proporcionan en la base de datos de Kaspersky Security Center y cuando los eventos se exportan a un sistema SIEM.
- **Descripción**. Un texto en el que se describen las situaciones en las que ocurren un evento y las acciones que se pueden tomar en cada caso.
- **Plazo de almacenamiento predeterminado**. El número de días por los que cada evento queda almacenado en la base de datos del Servidor de administración. Este es, también, el tiempo por el que el evento aparece en la lista de eventos del Servidor de administración. Transcurrido este período, el evento se elimina. Cuando el plazo de almacenamiento es 0, el evento se detecta, pero no se lo muestra en la lista de eventos del Servidor de administración. Si se configuró para guardar dichos eventos en el registro de eventos del sistema operativo, puede encontrarlos allí.

  Puede cambiar el plazo de almacenamiento para eventos:

  - Consola de administración: Configuración del plazo de almacenamiento para un evento
  - Kaspersky Security Center Web Console: Configuración del plazo de almacenamiento para un evento

Otros datos pueden incluir los siguientes campos:

- **event_id**: número único del evento en la base de datos, generado y asignado automáticamente; no se debe confundir con el **ID del tipo de evento**.
- **task_id**: el ID de la tarea que causó el evento (si lo hay).
- **gravedad**: uno de los siguientes niveles de gravedad (en orden ascendente de gravedad):

  0) Nivel de gravedad no válido

  1) Info.

  2) Advertencia

  3) Error

  4) Crítico

## Eventos del Servidor de administración

En esta sección, se brinda información sobre los eventos relacionados con el Servidor de administración.

## Eventos del Servidor de administración: nivel Crítico

En la siguiente tabla, se enumeran los tipos de eventos del Servidor de administración de Kaspersky Security Center que tienen el nivel de importancia **Crítico**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Para el Servidor de administración, también puede ver y configurar la lista de eventos en las propiedades del Servidor de administración. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Si especificó el puerto en la ventana de propiedades del Servidor de administración en la Consola de administración, **Kaspersky Security Center publica las métricas** y los eventos críticos que debe obtener Prometheus, un sistema de supervisión y alerta. Prometheus obtiene las métricas y los eventos críticos y, luego, genera alertas para cada evento.

// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Se ha superado el límite de la licencia** | 4099 | KLSRV_EV_LICENSE_CHECK_MORE_110 | Una vez al día, Kaspersky Security Center comprueba si se superó algún límite de licencia.<br>Este tipo de evento ocurre cuando el Servidor de administración detecta que las aplicaciones de Kaspersky instaladas en los dispositivos cliente han superado algún límite de sus licencias y se ha utilizado más de un 110 % del total de unidades con licencia cubiertas por una sola licencia.<br>Los dispositivos cliente se mantienen protegidos aun cuando ocurre este evento.<br>Puede responder al evento de los siguientes modos:<br>• Revise la lista de dispositivos administrados. Elimine los dispositivos que no estén en uso.<br>• Agregue una licencia para más dispositivos (agregue un código de activación válido o un archivo de clave en el Servidor de administración).<br>Kaspersky Security Center determina las reglas para generar eventos cuando se supera un límite de licencia. | 180 días |
| **Brote de virus** | 26 (para Protección contra archivos peligrosos) | GNRL_EV_VIRUS_OUTBREAK | Los eventos de este tipo ocurren cuando el número de objetos maliciosos detectados en varios dispositivos administrados supera el umbral en un corto período de tiempo.<br>Puede responder al evento de los siguientes modos:<br>• Configure el umbral en las propiedades del Servidor de administración.<br>• Cree una directiva más estricta que se active cuando ocurra este evento (o, como alternativa, cree una tarea que se ejecute cuando ocurra el evento). | 180 días |
| **Brote de virus** | 27 (para Protección contra amenazas de correo) | GNRL_EV_VIRUS_OUTBREAK | Los eventos de este tipo ocurren cuando el número de objetos maliciosos detectados en varios dispositivos administrados supera el umbral en un corto período de tiempo.<br>Puede responder al evento de los siguientes modos:<br>• Configure el umbral en las propiedades del Servidor de administración.<br>• Cree una directiva más estricta que se active cuando ocurra este evento (o, como alternativa, cree una tarea que se ejecute cuando ocurra el evento). | 180 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Brote de virus** | 28 (para el firewall) | GNRL_EV_VIRUS_OUTBREAK | Los eventos de este tipo ocurren cuando el número de objetos maliciosos detectados en varios dispositivos administrados supera el umbral en un corto período de tiempo.<br>Puede responder al evento de los siguientes modos:<br>• Configure el umbral en las propiedades del Servidor de administración.<br>• Cree una directiva más estricta que se active cuando ocurra este evento (o, como alternativa, cree una tarea que se ejecute cuando ocurra el evento). | 180 días |
| **El dispositivo ha cambiado a no administrado** | 4111 | KLSRV_HOST_OUT_CONTROL | Este tipo de eventos ocurren si un dispositivo administrado es visible en la red pero no se ha conectado al Servidor de administración durante un período específico.<br>Averigüe qué impide el correcto funcionamiento del Agente de red en el dispositivo. El problema podría deberse a un inconveniente en la red, por ejemplo, o al hecho de que el Agente de red se haya eliminado del dispositivo. | 180 días |
| **El estado del dispositivo es Crítico** | 4113 | KLSRV_HOST_STATUS_CRITICAL | Este tipo de evento ocurre cuando se le asigna el estado *Crítico* a un dispositivo administrado. Puede configurar las condiciones bajo las cuales el estado del dispositivo se cambia a *Crítico*. | 180 días |
| **El archivo de clave está en la lista de claves rechazadas** | 4124 | KLSRV_LICENSE_BLACKLISTED | Este tipo de evento ocurre cuando Kaspersky ha agregado el código de activación o el archivo de clave utilizados a la lista de rechazados.<br>Comuníquese con nuestro servicio de soporte técnico para más información. | 180 días |
| **Modo de funcionalidad limitada** | 4130 | KLSRV_EV_LICENSE_SRV_LIMITED_MODE | Este tipo de evento ocurre cuando Kaspersky Security Center pasa a operar con sus funciones básicas, sin las características Administración de dispositivos móviles y Administración de vulnerabilidades y parches.<br>Las causas de este evento y las maneras de responder son las siguientes:<br>• El periodo de vigencia de la licencia ha caducado. Agregue una licencia que permita usar el modo de funcionalidad completa de Kaspersky Security Center (agregue un código de activación válido o un archivo de clave en el Servidor de administración).<br>• El Servidor de administración gestiona más dispositivos de los que permite el límite de la licencia. Mueva los dispositivos de los grupos de administración de un Servidor de administración a los grupos de administración de otro Servidor de administración (si el límite de licencia del otro Servidor de administración lo admite). | 180 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **La licencia está por caducar** | 4129 | KLSRV_EV_LICENSE_SRV_EXPIRE_SOON | Este tipo de evento ocurre cuando se acerca la fecha de caducidad de una licencia comercial.<br>Kaspersky Security Center verifica una vez al día si alguna licencia está próxima a caducar. Los eventos de este tipo se publican 30 días, 15 días, 5 días y 1 día antes de la fecha de caducidad de la licencia. El número de días no se puede modificar. Si el Servidor de administración se encuentra apagado el día especificado antes de la fecha de caducidad de la licencia, el evento no se publicará sino hasta el día siguiente.<br>Cuando caduca la licencia comercial, Kaspersky Security Center solo brinda acceso a las funciones básicas.<br>Puede responder al evento de los siguientes modos:<br>• Asegúrese de tener una clave de licencia de reserva agregada en el Servidor de administración.<br>• Si usa una suscripción, no olvide renovarla. Una suscripción ilimitada se renueva automáticamente si el proveedor de servicios recibe a término y por adelantado el pago correspondiente. | 180 días |
| **El certificado ha caducado** | 4132 | KLSRV_CERTIFICATE_EXPIRED | Los eventos de este tipo ocurren cuando caduca el certificado cliente en los dispositivos móviles. | 180 días |
| **El certificado del servidor de administración ha caducado.** | 6129 | ServerCertificateExpired | Este tipo de evento ocurre cuando caducan los certificados del Servidor de administración para los dispositivos móviles y dispositivos UEFI.<br>Deberá actualizar el certificado caducado. | 180 días |
| **Se revocaron las actualizaciones de los módulos de la aplicación de Kaspersky** | 4142 | KLSRV_SEAMLESS_UPDATE_REVOKED | Este tipo de evento ocurre cuando los especialistas técnicos de Kaspersky revocan una actualización sin interrupciones (tales actualizaciones tienen el estado *Revocada*) y resulta necesario, por ejemplo, actualizar a una versión más nueva. El evento afecta a los parches de Kaspersky Security Center, pero no a los módulos de las aplicaciones de Kaspersky administradas. La razón por la que no se instaló la actualización sin interrupciones se indica en el evento. | 180 días |
| **Auditoría: la exportación a SIEM produjo un error** | 5130 | KLAUD_EV_SIEM_EXPORT_ERROR | Los eventos de este tipo ocurren cuando la exportación de eventos al sistema SIEM falla debido a un error de conexión con el sistema SIEM. | 180 días |

## Eventos del Servidor de administración: nivel Error funcional

En la siguiente tabla, se enumeran los tipos de eventos del Servidor de administración de Kaspersky Security Center que tienen el nivel de importancia **Error funcional**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Para el Servidor de administración, también puede ver y configurar la lista de eventos en las propiedades del Servidor de administración. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Servidor de administración: nivel Error funcional

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Error en tiempo de ejecución** | 4125 | KLSRV_RUNTIME_ERROR | Los eventos de este tipo ocurren debido a problemas desconocidos.<br>En la mayoría de los casos, estos son problemas de DBMS, problemas de red y otros problemas de software y hardware.<br>Los detalles del evento se pueden encontrar en la descripción del evento. | 180 días |
| **Límite de instalaciones excedido en uno de los grupos de aplicaciones con licencia** | 4126 | KLSRV_INVLICPROD_EXCEDED | El Servidor de administración genera eventos de este tipo periódicamente (cada una hora). Los eventos de este tipo ocurren si administra claves de licencia de aplicaciones de terceros en Kaspersky Security Center y si el número de instalaciones ha superado el límite establecido por la clave de licencia de la aplicación de terceros.<br>Puede responder al evento de los siguientes modos:<br>• Revise la lista de dispositivos administrados. Si la aplicación del tercero no se está utilizando en algún dispositivo, desinstálela de ese equipo.<br>• Solicite al tercero una licencia para más dispositivos.<br>Para administrar las claves de licencia de sus aplicaciones de terceros, puede utilizar la característica de grupos de aplicaciones con licencia. Un grupo de aplicaciones con licencia está formado por aplicaciones de terceros que cumplen con los criterios que usted define. | 180 días |
| **Error al sondear el segmento de la nube** | 4143 | KLSRV_KLCLOUD_SCAN_ERROR | Los eventos de este tipo ocurren cuando el Servidor de administración no puede sondear un segmento de red en un entorno de nube. Lea los detalles en la descripción del evento y responda en consecuencia. | No se almacena |
| **Error al copiar las actualizaciones a la carpeta especificada** | 4123 | KLSRV_UPD_REPL_FAIL | Los eventos de este tipo se producen cuando las actualizaciones de software se copian en una carpeta compartida adicional.<br>Puede responder al evento de los siguientes modos:<br>• Verifique si la cuenta de usuario que se emplea para obtener acceso a la(s) carpeta(s) tiene permiso de escritura.<br>• Compruebe si se cambiaron nombre de usuario o contraseña de las carpetas.<br>• Compruebe la conexión a Internet, ya que podría ser la causa del evento. Siga las instrucciones para actualizar las bases de datos y los módulos de software. | 180 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **No queda espacio libre en disco** | 4107 | KLSRV_DISK_FULL | Los eventos de este tipo ocurren cuando el disco duro del dispositivo donde está instalado el Servidor de administración se queda sin espacio libre.<br>Libere espacio en el disco del dispositivo. | 180 días |
| **La carpeta compartida no está disponible** | 4108 | KLSRV_SHARED_FOLDER_UNAVAILABLE | Los eventos de este tipo se producen si la carpeta compartida del Servidor de administración no está disponible.<br>Puede responder al evento de los siguientes modos:<br>• Compruebe si el Servidor de administración (donde se encuentra la carpeta compartida) está encendido y disponible.<br>• Compruebe si se cambió/cambiaron un nombre de usuario y / o una contraseña de la carpeta.<br>• Compruebe la conexión de red. | 180 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **La base de datos del Servidor de administración no está disponible** | 4109 | KLSRV_DATABASE_UNAVAILABLE | Los eventos de este tipo ocurren si la base de datos del Servidor de administración deja de estar disponible.<br>Puede responder al evento de los siguientes modos:<br>• Compruebe si el servidor remoto que tiene instalado SQL Server está disponible.<br>• Vea los registros de DBMS para descubrir el motivo de la falta de disponibilidad de la base de datos del Servidor de administración. Por ejemplo, debido al mantenimiento preventivo, un servidor remoto con SQL Server instalado puede no estar disponible. | 180 días |
| **No hay espacio libre en la base de datos del Servidor de administración** | 4110 | KLSRV_DATABASE_FULL | Los eventos de este tipo ocurren cuando no hay espacio libre en la base de datos del Servidor de administración.<br>El Servidor de administración no funciona cuando su base de datos ha alcanzado su capacidad y cuando no es posible realizar un nuevo registro en la base de datos.<br>Las siguientes son las causas de este evento (agrupadas por DBMS) y distintas maneras en las que puede responder al mismo:<br>• Si su DBMS es SQL Server Express Edition:<br>En la documentación de SQL Server Express, revise el límite de tamaño de la base de datos de la versión que usa. Probablemente su base de datos del Servidor de administración haya excedido el límite de tamaño de la base de datos.<br>Limite el número de eventos que se almacenan en la base de datos del Servidor de administración.<br>La base de datos del Servidor de administración contiene demasiados eventos enviados por el componente Control de aplicaciones. Puede cambiar la configuración de la directiva de Kaspersky Endpoint Security para Windows relacionada con el almacenamiento de eventos de Control de aplicaciones en la base de datos del Servidor de administración.<br>• Si su DBMS no es SQL Server Express Edition:<br>No limite el número de eventos para almacenar en la base de datos del Servidor de administración.<br>Reduzca la lista de eventos para almacenar en la base de datos del Servidor de administración.<br>Revise la información sobre la selección del DBMS. | 180 días |

## Eventos del Servidor de administración: nivel Advertencia

En la siguiente tabla, se enumeran los eventos del Servidor de administración de Kaspersky Security Center que tienen el nivel de importancia **Advertencia**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Para el Servidor de administración, también puede ver y configurar la lista de eventos en las propiedades del Servidor de administración. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Servidor de administración: nivel Advertencia

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Se detectó un evento frecuente** | | KLSRV_EVENT_SPAM_EVENTS_DETECTED | Este tipo de evento ocurre cuando el Servidor de administración detecta un evento frecuente en un dispositivo administrado. Consulte la siguiente sección para obtener más información: Bloquear eventos frecuentes. | 90 días |
| **Se ha superado el límite de la licencia** | 4098 | KLSRV_EV_LICENSE_CHECK_100_110 | Una vez al día, Kaspersky Security Center comprueba si se superó algún límite de licencia.<br>Este tipo de evento ocurre cuando el Servidor de administración detecta que las aplicaciones de Kaspersky instaladas en los dispositivos cliente han superado algún límite de sus licencias y se ha utilizado entre un 100 % y un 110 % del total de unidades con licencia cubiertas por una sola licencia.<br>Los dispositivos cliente se mantienen protegidos aun cuando ocurre este evento.<br>Puede responder al evento de los siguientes modos:<br>• Revise la lista de dispositivos administrados. Elimine los dispositivos que no estén en uso.<br>• Agregue una licencia para más dispositivos (agregue un código de activación válido o un archivo de clave en el Servidor de administración).<br>Kaspersky Security Center determina las reglas para generar eventos cuando se supera un límite de licencia. | 90 días |
| **El dispositivo ha estado inactivo en la red por mucho tiempo** | 4103 | KLSRV_EVENT_HOSTS_NOT_VISIBLE | Este tipo de evento ocurre cuando un dispositivo administrado se encuentra inactivo durante cierto tiempo.<br>La mayoría de las veces, esto sucede porque el dispositivo se ha dado de baja.<br>Puede responder al evento de los siguientes modos:<br>• Elimine el dispositivo manualmente de la lista de dispositivos administrados.<br>• Defina el intervalo de tiempo después del cual se creará el evento **El dispositivo ha estado inactivo en la red por mucho tiempo** mediante la Consola de administración o Kaspersky Security Center Web Console.<br>• Defina el intervalo de tiempo después del cual el dispositivo se eliminará automáticamente del grupo mediante la Consola de administración o Kaspersky Security Center Web Console. | 90 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Conflicto de nombres de dispositivo** | 4102 | KLSRV_EVENT_HOSTS_CONFLICT | Este tipo de evento ocurre cuando el Servidor de administración considera que dos o más dispositivos administrados son un mismo dispositivo.<br>A menudo, esto sucede cuando se utiliza un disco duro clonado para desplegar aplicaciones en los dispositivos administrados, pero el Agente de red del dispositivo de referencia no estaba puesto en el modo de clonación de disco dedicado.<br>Para evitar este problema, ponga el Agente de red en modo de clonación de disco en el dispositivo de referencia antes de clonar el disco duro de ese dispositivo. | 90 días |
| **El estado del dispositivo es Advertencia** | 4114 | KLSRV_HOST_STATUS_WARNING | Este tipo de evento ocurre cuando se le asigna el estado *Advertencia* a un dispositivo administrado. Puede configurar las condiciones en las cuales el estado del dispositivo se cambia a *Advertencia*. | 90 días |
| **El límite de instalaciones está por excederse en uno de los grupos de aplicaciones con licencia** | 4127 | KLSRV_INVLICPROD_FILLED | Este tipo de evento ocurre cuando el número de instalaciones para las aplicaciones de terceros incluidas en un grupo de aplicaciones con licencia alcanza el 90 % del valor máximo permitido en las propiedades de la clave de licencia.<br>Puede responder al evento de los siguientes modos:<br>• Si la aplicación de terceros no se utiliza en algunos de los dispositivos administrados, elimínela de esos dispositivos.<br>• Si estima que la cantidad de instalaciones para la aplicación de terceros superará el máximo permitido en un futuro próximo, considere contactarse con el tercero antes de que eso suceda para obtener una licencia para una cantidad de dispositivos mayor.<br>Para administrar las claves de licencia de sus aplicaciones de terceros, puede utilizar la característica de grupos de aplicaciones con licencia. | 90 días |
| **Se solicitó el certificado** | 4133 | KLSRV_CERTIFICATE_REQUESTED | Este tipo de evento ocurre cuando un certificado de la característica Administración de dispositivos móviles no se vuelve a emitir automáticamente.<br>Estas pueden ser las causas del evento y las respuestas adecuadas:<br>• Se intentó reemitir automáticamente un certificado para el que estaba deshabilitada la opción **Volver a emitir certificados automáticamente si es posible**. Esto puede deberse a un error ocurrido durante la creación del certificado. Es posible que se requiera la reemisión manual del certificado.<br>• Si ha configurado la integración con una infraestructura de claves públicas, la causa podría ser la falta de un atributo SAM-Account-Name de la cuenta utilizada para la integración con dicha infraestructura y para la emisión del certificado. Revise las propiedades de la cuenta. | 90 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Se eliminó el certificado** | 4134 | KLSRV_CERTIFICATE_REMOVED | Este tipo de evento ocurre cuando un administrador elimina un certificado de cualquier tipo (general, de correo o de VPN) para Administración de dispositivos móviles.<br>Después de que se elimina un certificado, los dispositivos móviles que lo habían utilizado para conectarse pierden la capacidad de establecer conexión con el Servidor de administración.<br>Este evento puede resultar útil a la hora de investigar fallas asociadas con la administración de dispositivos móviles. | 90 días |
| **El certificado está por caducar.** | 6128 | ServerCertificateExpiresSoon | Este tipo de evento ocurre cuando caducan los certificados del Servidor de administración para los dispositivos móviles y dispositivos UEFI.<br>Deberá actualizar el certificado caducado. | 90 días |
| **El certificado de APNs caducó** | 4135 | KLSRV_APN_CERTIFICATE_EXPIRED | Este tipo de evento ocurre cuando caduca un certificado de APNs.<br>Debe renovar manualmente el certificado de APNs e instalarlo en un servidor de MDM para iOS. | No se almacena |
| **El certificado de APNs caducará pronto** | 4136 | KLSRV_APN_CERTIFICATE_EXPIRES_SOON | Este tipo de evento ocurre cuando quedan menos de catorce días para que caduque el certificado de APNs.<br>Cuando el certificado de APNs caduque, deberá renovarlo manualmente e instalarlo en un servidor de MDM para iOS.<br>Le recomendamos que programe la renovación del certificado de APNs para antes de la fecha de caducidad. | No se almacena |
| **No se pudo enviar el mensaje de FCM al dispositivo móvil** | 4138 | KLSRV_GCM_DEVICE_ERROR | Los eventos de este tipo ocurren cuando la Administración de dispositivos móviles está configurada para usar Firebase Cloud Messaging (FCM) para conectarse a dispositivos móviles administrados con un sistema operativo Android y el servidor de FCM no puede manejar algunas de las solicitudes recibidas del Servidor de administración. Lo que esto significa es que algunos de los dispositivos móviles administrados no recibirán una notificación push.<br>Lea el código HTTP en los detalles de la descripción del evento y responda en consecuencia. Para obtener más información sobre los códigos HTTP recibidos del servidor de FCM y los errores relacionados, consulte la documentación del servicio Firebase (en especial, el capítulo "Códigos de respuesta de errores de mensajes descendentes"). | 90 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Error de HTTP al enviar un mensaje del FCM al servidor de FCM** | 4139 | KLSRV_GCM_HTTP_ERROR | Los eventos de este tipo ocurren cuando la Administración de dispositivos móviles está configurada para usar Firebase Cloud Messaging (FCM) para conectar dispositivos móviles administrados con el sistema operativo Android y el servidor de FCM devuelve al Servidor de administración una solicitud con un código HTTP distinto de 200 (OK).<br>Estas pueden ser las causas del evento y las respuestas adecuadas:<br>• Problemas en el servidor de FCM. Lea el código HTTP en los detalles de la descripción del evento y responda en consecuencia. Para obtener más información sobre los códigos HTTP recibidos del servidor de FCM y los errores relacionados, consulte la documentación del servicio Firebase (en especial, el capítulo "Códigos de respuesta de errores de mensajes descendentes").<br>• Problemas en el servidor proxy (si usa un servidor proxy). Lea el código HTTP en los detalles de la descripción del evento y responda en consecuencia. | 90 días |
| **No se pudo enviar el mensaje de FCM al servidor de FCM** | 4140 | KLSRV_GCM_GENERAL_ERROR | Este tipo de evento ocurre cuando suceden errores inesperados del lado del Servidor de administración al utilizar el protocolo HTTP de Firebase Cloud Messaging.<br>Lea los detalles en la descripción del evento y responda en consecuencia.<br>Si no puede encontrar la solución a un problema por su cuenta, le recomendamos que se comunique con el servicio de soporte técnico de Kaspersky. | 90 días |
| **Queda poco espacio libre en el disco duro** | 4105 | KLSRV_NO_SPACE_ON_VOLUMES | Este tipo de evento ocurre cuando se agota el espacio en el disco duro del dispositivo en el que está instalado el Servidor de administración.<br>Libere espacio en el disco del dispositivo. | 90 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Queda poco espacio libre en la base de datos del Servidor de administración** | 4106 | KLSRV_NO_SPACE_IN_DATABASE | Este tipo de evento ocurre cuando el espacio disponible en la base de datos del Servidor de administración es demasiado limitado. De no resolverse esta situación, la base de datos del Servidor de administración alcanzará rápidamente su límite de capacidad y el Servidor de la administración dejará de funcionar.<br>Las siguientes son las causas de este evento (agrupadas por DBMS) y las distintas maneras en las que puede responder.<br>Si su DBMS es SQL Server Express Edition:<br>• En la documentación de SQL Server Express, revise el límite de tamaño de la base de datos de la versión que usa. Es probable que la base de datos del Servidor de administración esté a punto de alcanzar el tamaño máximo posible.<br>• Limite el número de eventos que se almacenan en la base de datos del Servidor de administración.<br>• La base de datos del Servidor de administración contiene demasiados eventos enviados por el componente Control de aplicaciones. Puede cambiar la configuración de la directiva de Kaspersky Endpoint Security para Windows relacionada con el almacenamiento de eventos de Control de aplicaciones en la base de datos del Servidor de administración.<br>Si su DBMS no es SQL Server Express Edition:<br>• No limite el número de eventos que se almacenan en la base de datos del Servidor de administración.<br>• Reduzca la lista de eventos que se almacenan en la base de datos del Servidor de administración.<br>Revise la información sobre la selección del DBMS. | 90 días |
| **Se ha interrumpido la conexión con el Servidor de administración secundario** | 4116 | KLSRV_EV_SLAVE_SRV_DISCONNECTED | Este tipo de evento ocurre cuando se interrumpe una conexión con el Servidor de administración secundario.<br>Consulte el registro de eventos de Kaspersky en el dispositivo en el que esté instalado el Servidor de administración secundario y responda en consecuencia. | 90 días |
| **Se ha interrumpido la conexión con el Servidor de administración principal** | 4118 | KLSRV_EV_MASTER_SRV_DISCONNECTED | Este tipo de evento ocurre cuando se interrumpe una conexión con el Servidor de administración principal.<br>Consulte el registro de eventos de Kaspersky en el dispositivo en el que esté instalado el Servidor de administración principal y responda en consecuencia. | 90 días |
| **Se registraron nuevas actualizaciones para los módulos de la aplicación de Kaspersky** | 4141 | KLSRV_SEAMLESS_UPDATE_REGISTERED | Este tipo de evento ocurre cuando el Servidor de administración registra nuevas actualizaciones para el software de Kaspersky instalado en los dispositivos administrados y se necesita que usted apruebe la instalación de esas actualizaciones.<br>Apruebe o rechace las actualizaciones mediante la Consola de administración o a través de Kaspersky Security Center Web Console. | 90 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Se superó el límite del número de eventos en la base de datos, se inició la eliminación de eventos** | 4145 | KLSRV_EVP_DB_TRUNCATING | Este tipo de evento ocurre cuando el sistema comienza a eliminar eventos antiguos de la base de datos del Servidor de administración por haberse alcanzado el límite de capacidad de la misma.<br>Puede responder al evento de los siguientes modos:<br>• Cambie el número de eventos que se conservará, como máximo, en la base de datos del Servidor de administración.<br>• Reduzca la lista de eventos que se almacenan en la base de datos del Servidor de administración. | No se almacena |
| **Se superó el límite del número de eventos en la base de datos, se eliminó los eventos** | 4146 | KLSRV_EVP_DB_TRUNCATED | Este tipo de evento ocurre cuando el sistema eliminó eventos antiguos de la base de datos del Servidor de administración por haberse alcanzado el límite de capacidad de la misma.<br>Puede responder al evento de los siguientes modos:<br>• Cambie el número de eventos que se conservará, como máximo, en la base de datos del Servidor de administración.<br>• Reduzca la lista de eventos que se almacenan en la base de datos del Servidor de administración. | No se almacena |
| **Auditoría (la prueba de conexión al servidor de SIEM produjo un error)** | 5120 | KLAUD_EV_SIEM_TEST_FAILED | Los eventos de este tipo se producen cuando falla una conexión de prueba al servidor SIEM. | 30 días |
| **No se pudo emitir el certificado automáticamente** | | KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR | Este evento ocurre en caso de un error al crear un certificado de cliente para un dispositivo móvil (un dispositivo que opera bajo un protocolo móvil). | 90 días |

## Eventos del Servidor de administración: nivel Información

En la siguiente tabla, se enumeran los eventos del Servidor de administración de Kaspersky Security Center que tienen el nivel de importancia **Información**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Para el Servidor de administración, también puede ver y configurar la lista de eventos en las propiedades del Servidor de administración. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Servidor de administración: nivel Información

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado | Observaciones |
|---|---|---|---|---|
| **Se ha consumido más del 90 % de la clave de licencia** | 4097 | KLSRV_EV_LICENSE_CHECK_90 | 30 días | |
| **Se detectó un nuevo dispositivo** | 4100 | KLSRV_EVENT_HOSTS_NEW_DETECTED | 30 días | |
| **Dispositivo agregado al grupo automáticamente** | 4101 | KLSRV_EVENT_HOSTS_NEW_REDIRECTED | 30 días | |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado | Observaciones |
|---|---|---|---|---|
| **El dispositivo se movió automáticamente de acuerdo con una regla** | 1074 | KLSRV_HOST_MOVED_WITH_RULE_EX | 30 días | |
| **Dispositivo eliminado del grupo: estuvo inactivo en la red por mucho tiempo** | 4104 | KLSRV_INVISIBLE_HOSTS_REMOVED | 30 días | |
| **El límite de instalaciones está por alcanzarse (se consumió más del 95 %) en uno de los grupos de aplicaciones con licencia** | 4128 | KLSRV_INVLICPROD_EXPIRED_SOON | 30 días | |
| **Se han encontrado archivos para enviar a Kaspersky para su análisis** | 4131 | KLSRV_APS_FILE_APPEARED | 30 días | |
| **El id. de instancia de FCM ha cambiado en este dispositivo móvil** | 4137 | KLSRV_GCM_DEVICE_REGID_CHANGED | 30 días | |
| **Las actualizaciones se copiaron correctamente en la carpeta especificada** | 4122 | KLSRV_UPD_REPL_OK | 30 días | |
| **Se estableció la conexión con el Servidor de administración secundario** | 4115 | KLSRV_EV_SLAVE_SRV_CONNECTED | 30 días | |
| **Se estableció la conexión con el Servidor de administración principal** | 4117 | KLSRV_EV_MASTER_SRV_CONNECTED | 30 días | |
| **Las bases de datos se han actualizado** | 4144 | KLSRV_UPD_BASES_UPDATED | 30 días | |
| **Auditoría: Se estableció la conexión con el Servidor de administración** | 4147 | KLAUD_EV_SERVERCONNECT | 30 días | Los eventos de este tipo ocurren cuando un usuario se conecta al Servidor de administración mediante la Consola de administración o Kaspersky Security Center Web Console. Estos eventos incluyen información sobre la dirección IP del dispositivo donde está instalado el Servidor de Kaspersky Security Center Web Console o la Consola de administración basada en MMC. |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado | Observaciones |
|---|---|---|---|---|
| **Auditoría: El objeto se modificó** | 4148 | KLAUD_EV_OBJECTMODIFY | 30 días | Este evento responde a cambios ocurridos en los siguientes objetos:<br>• Grupo de administración<br>• Grupo de seguridad<br>• Usuario<br>• Paquete<br>• Tarea<br>• Directiva<br>• Servidores<br>• Servidor virtual |
| **Auditoría: El estado del objeto se modificó** | 4150 | KLAUD_EV_TASK_STATE_CHANGED | 30 días | Este evento ocurre, por ejemplo, cuando una tarea no se completa debido a un error. |
| **Auditoría: La configuración del grupo se modificó** | 4149 | KLAUD_EV_ADMGROUP_CHANGED | 30 días | |
| **Auditoría: Se cerró la conexión con el Servidor de administración** | 4151 | KLAUD_EV_SERVERDISCONNECT | 30 días | |
| **Auditoría: Las propiedades del objeto se han modificado** | 4152 | KLAUD_EV_OBJECTPROPMODIFIED | 30 días | Este evento responde a cambios ocurridos en las siguientes propiedades:<br>• Usuario<br>• Licencia<br>• Servidores<br>• Servidor virtual |
| **Auditoría: Las propiedades del usuario se han modificado** | 4153 | KLAUD_EV_OBJECTACLMODIFIED | 30 días | |
| **Auditoría: Se importaron o exportaron claves de cifrado del Servidor de administración** | 5100 | KLAUD_EV_DPEKEYSEXPORT | 30 días | |
| **Auditoría: la prueba de conexión al servidor de SIEM se realizó correctamente** | 5110 | KLAUD_EV_SIEM_TEST_SUCCESS | 30 días | Los eventos de este tipo se producen cuando se logra establecer una conexión de prueba con el servidor SIEM. |
| **Certificado de reserva creado** | | ServerReserveCertificateCreated | 30 días | Este evento se produce cuando se crea un certificado del Servidor de administración. |
| **Renovación del certificado** | | ServerCertificateRenewed | 30 días | Este evento ocurre cuando se renueva el certificado del Servidor de administración. |

Los eventos **Certificado de reserva creado** y **Renovación del certificado** son publicados automáticamente por el Servidor de administración y se muestran en la Consola de administración solo cuando las operaciones

correspondientes a estos eventos se realizan para los certificados del Servidor de administración para dispositivos con certificado móvil y dispositivos UEFI.

## Eventos del Agente de red

En esta sección, se brinda información sobre los eventos relacionados con el Agente de red.

## Eventos del Agente de red: nivel Error funcional

En la siguiente tabla, se enumeran los tipos de eventos del Agente de red de Kaspersky Security Center que tienen el nivel de gravedad **Error funcional**.

Puede definir los ajustes de notificación y los ajustes de almacenamiento para cada uno de los eventos que pueda generar una aplicación; para ello debe dirigirse a la pestaña **Configuración de eventos** en la directiva de la aplicación. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Agente de red: nivel Error funcional

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **Error de instalación de la actualización** | 7702 | KLNAG_EV_PATCH_INSTALL_ERROR | Los eventos de este tipo se producen si la actualización automática y la aplicación de parches para los componentes de Kaspersky Security Center no tuvieron éxito. El evento no está vinculado a la actualización de las aplicaciones de Kaspersky administradas.<br>Lea la descripción del evento. El evento puede tener su origen en un problema de Windows ocurrido en el Servidor de administración. Si la descripción menciona algún problema con la configuración de Windows, resuelva ese problema. | 30 días |
| **Error al instalar la actualización de software de terceros** | 7697 | KLNAG_EV_3P_PATCH_INSTALL_ERROR | Los eventos de este tipo se producen si las funciones de Administración de vulnerabilidades y parches y Administración de dispositivos móviles están en uso y si la actualización del software de terceros no se realizó correctamente.<br>Compruebe si el enlace al software desarrollado por el tercero es válido. Lea la descripción del evento. | 30 días |
| **Error al instalar las actualizaciones de Windows Update** | 7717 | KLNAG_EV_WUA_INSTALL_ERROR | Este tipo de evento ocurre cuando no se pueden instalar las actualizaciones de Windows. Configurar las actualizaciones de Windows en una directiva del Agente de red.<br>Lea la descripción del evento. Busque el error en Microsoft Knowledge Base. Póngase en contacto con el servicio de soporte técnico de Microsoft si no puede resolver el problema por su cuenta. | 30 días |
| **Administración de usuarios: errores** | 7723 | KLNAG_EV_USR_MNG_ERR | Evento de advertencia general. | 30 días |
| **No se pudo restaurar el archivo sudoers al valor de referencia** | 7726 | KLNAG_EV_SUDOER_RESTORED_ERR | El evento contiene la descripción correspondiente al error de reemplazo del archivo sudoers. | 30 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Descripción | Plazo de almacenamiento predeterminado |
|---|---|---|---|---|
| **No se pudieron instalar los certificados raíz** | 7728 | KLNAG_EV_ROOT_CERT_INSTALL_ERR | El evento contiene la descripción correspondiente al error de instalación de los certificados. | 30 días |
| **No se pudieron eliminar los certificados raíz** | 7730 | KLNAG_EV_ROOT_CERT_REMOVE_ERR | El evento contiene la descripción correspondiente al error de eliminación de certificados. | 30 días |

## Eventos del Agente de red: nivel Advertencia

La siguiente tabla muestra los eventos del Agente de red de Kaspersky Security Center Linux que tienen el nivel de gravedad **Advertencia**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Agente de red: nivel Advertencia

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado |
|---|---|---|---|
| **Se ha devuelto una advertencia durante la instalación de la actualización del módulo de software** | 7701 | KLNAG_EV_PATCH_INSTALL_WARNING | 30 días |
| **La instalación de la actualización de software de terceros se ha completado con una advertencia** | 7696 | KLNAG_EV_3P_PATCH_INSTALL_WARNING | 30 días |
| **La instalación de la actualización de software de terceros se ha pospuesto** | 7698 | KLNAG_EV_3P_PATCH_INSTALL_SLIPPED | 30 días |
| **Ocurrió un problema de seguridad** | 549 | GNRL_EV_APP_INCIDENT_OCCURED | 30 días |
| **Se inició el Proxy de KSN. No se pudo comprobar la disponibilidad de KSN** | 7718 | KSNPROXY_STARTED_CON_CHK_FAILED | 30 días |
| **Administración de usuarios: advertencias** | 7722 | KLNAG_EV_USR_MNG_WRN | 30 días |
| **El archivo sudoers encontrado no coincide con el valor de referencia** | 7724 | KLNAG_EV_SUDOER_DIFFERENT | 30 días |

## Eventos del Agente de red: nivel Información

La siguiente tabla muestra los eventos del Agente de red de Kaspersky Security Center Linux que tienen el nivel de gravedad **Información**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Agente de red: nivel Información

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado |
|---|---|---|---|
| **La actualización para los módulos de software se instaló correctamente** | 7699 | KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY | 30 días |
| **Se ha iniciado la instalación de la actualización para los módulos de software** | 7700 | KLNAG_EV_PATCH_INSTALL_STARTING | 30 días |
| **Se instaló una aplicación** | 7703 | KLNAG_EV_INV_APP_INSTALLED | 30 días |
| **Se desinstaló una aplicación** | 7704 | KLNAG_EV_INV_APP_UNINSTALLED | 30 días |

| Nombre que se muestra para el tipo de evento | Id. del tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado |
|---|---|---|---|
| **Se instaló una aplicación supervisada** | 7705 | KLNAG_EV_INV_OBS_APP_INSTALLED | 30 días |
| **Se desinstaló una aplicación supervisada** | 7706 | KLNAG_EV_INV_OBS_APP_UNINSTALLED | 30 días |
| **Se instaló una aplicación de terceros** | 7707 | KLNAG_EV_INV_CMPTR_APP_INSTALLED | 30 días |
| **Nuevo dispositivo agregado** | 7708 | KLNAG_EV_DEVICE_ARRIVAL | 30 días |
| **Dispositivo eliminado** | 7709 | KLNAG_EV_DEVICE_REMOVE | 30 días |
| **Se detectó un nuevo dispositivo** | 7710 | KLNAG_EV_NAC_DEVICE_DISCOVERED | 30 días |
| **Dispositivo autorizado** | 7711 | KLNAG_EV_NAC_HOST_AUTHORIZED | 30 días |
| **Windows Desktop Sharing: el archivo ha sido leído** | 7712 | KLUSRLOG_EV_FILE_READ | 30 días |
| **Windows Desktop Sharing: el archivo ha sido modificado** | 7713 | KLUSRLOG_EV_FILE_MODIFIED | 30 días |
| **Windows Desktop Sharing: la aplicación ha sido iniciada** | 7714 | KLUSRLOG_EV_PROCESS_LAUNCHED | 30 días |
| **Windows Desktop Sharing: iniciado** | 7715 | KLUSRLOG_EV_WDS_BEGIN | 30 días |
| **Windows Desktop Sharing: detenido** | 7716 | KLUSRLOG_EV_WDS_END | 30 días |
| **La actualización de software de terceros se ha instalado correctamente** | 7694 | KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY | 30 días |
| **Se ha iniciado la instalación de la actualización de software de terceros** | 7695 | KLNAG_EV_3P_PATCH_INSTALL_STARTING | 30 días |
| **El proxy de KSN se ha iniciado. La disponibilidad de KSN se verificó correctamente** | 7719 | KSNPROXY_STARTED_CON_CHK_OK | 30 días |
| **El Proxy de KSN se detuvo** | 7720 | KSNPROXY_STOPPED | 30 días |

## Eventos del Servidor de MDM para iOS

Esta sección contiene información sobre los eventos relacionados con el Servidor de MDM para iOS.

## Eventos de errores funcionales del Servidor de MDM para iOS

La siguiente tabla muestra los eventos del servidor de MDM para iOS de Kaspersky Security Center que tienen el nivel de gravedad **Error funcional**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos de errores funcionales del Servidor de MDM para iOS

| Nombre que se muestra para el tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado |
|---|---|---|
| **Error al solicitar la lista de perfiles** | PROFILELIST_COMMAND_FAILED | 30 días |
| **Error al instalar perfil** | INSTALLPROFILE_COMMAND_FAILED | 30 días |
| **Error al eliminar el perfil** | REMOVEPROFILE_COMMAND_FAILED | 30 días |
| **Error al solicitar la lista de perfiles de aprovisionamiento** | PROVISIONINGPROFILELIST_COMMAND_FAILED | 30 días |
| **Error al instalar perfil de aprovisionamient** | INSTALLPROVISIONINGPROFILE_COMMAND_FAILED | 30 días |
| **Error al eliminar perfil de aprovisionamiento** | REMOVEPROVISIONINGPROFILE_COMMAND_FAILED | 30 días |

| Nombre que se muestra para el tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado |
|---|---|---|
| **Error al solicitar la lista de certificados digitales** | CERTIFICATELIST_COMMAND_FAILED | 30 días |
| **Error al solicitar la lista de aplicaciones instaladas** | INSTALLEDAPPLICATIONLIST_COMMAND_FAILED | 30 días |
| **Error al solicitar información general sobre el dispositivo móvil** | DEVICEINFORMATION_COMMAND_FAILED | 30 días |
| **Error al solicitar la información de seguridad** | SECURITYINFO_COMMAND_FAILED | 30 días |
| **No se pudo bloquear el dispositivo móvil** | DEVICELOCK_COMMAND_FAILED | 30 días |
| **Error al restablecer la contraseña** | CLEARPASSCODE_COMMAND_FAILED | 30 días |
| **Error al eliminar los datos del dispositivo móvil** | ERASEDEVICE_COMMAND_FAILED | 30 días |
| **No se pudo instalar la app** | INSTALLAPPLICATION_COMMAND_FAILED | 30 días |
| **Error al establecer el código de canje para la app** | APPLYREDEMPTIONCODE_COMMAND_FAILED | 30 días |
| **Error al solicitar la lista de apps administradas** | MANAGEDAPPLICATIONLIST_COMMAND_FAILED | 30 días |
| **No se pudo eliminar la app administrada** | REMOVEAPPLICATION_COMMAND_FAILED | 30 días |
| **La configuración de roaming se ha rechazado** | SETROAMINGSETTINGS_COMMAND_FAILED | 30 días |
| **Se produjo un error en la operación de la app** | PRODUCT_FAILURE | 30 días |
| **El resultado del comando contiene datos no válidos** | MALFORMED_COMMAND | 30 días |
| **Error al enviar la notificación push** | SEND_PUSH_NOTIFICATION_FAILED | 30 días |
| **No se puede enviar el comando** | SEND_COMMAND_FAILED | 30 días |
| **Dispositivo no encontrado** | DEVICE_NOT_FOUND | 30 días |

## Eventos de advertencia del servidor de MDM para iOS

La siguiente tabla muestra los eventos del servidor de MDM para iOS de Kaspersky Security Center que tienen el nivel de gravedad **Advertencia**.

Puede definir los ajustes de notificación y los ajustes de almacenamiento para cada uno de los eventos que pueda generar una aplicación; para ello debe dirigirse a la pestaña **Configuración de eventos** en la directiva de la aplicación. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos de advertencia del servidor de MDM para iOS

| Nombre que se muestra para el tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado |
|---|---|---|
| **Se detectó un intento de conectar un dispositivo móvil bloqueado** | INACTICE_DEVICE_TRY_CONNECTED | 30 días |
| **El perfil se ha eliminado** | MDM_PROFILE_WAS_REMOVED | 30 días |
| **Se detectó un intento de reutilizar un certificado cliente** | CLIENT_CERT_ALREADY_IN_USE | 30 días |
| **Se detectó un dispositivo inactivo** | FOUND_INACTIVE_DEVICE | 30 días |
| **Se requiere el código de canje** | NEED_REDEMPTION_CODE | 30 días |
| **El perfil incluido en la directiva se ha eliminado del dispositivo** | UMDM_PROFILE_WAS_REMOVED | 30 días |

## Eventos informativos del servidor de MDM para iOS

La siguiente tabla muestra los eventos del servidor de MDM para iOS de Kaspersky Security Center que tienen el nivel de gravedad **Información**.

Puede definir los ajustes de notificación y los ajustes de almacenamiento para cada uno de los eventos que pueda generar una aplicación; para ello debe dirigirse a la pestaña **Configuración de eventos** en la directiva de la aplicación. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos informativos del servidor de MDM para iOS

| Nombre que se muestra para el tipo de evento | Tipo de evento | Plazo de almacenamiento predeterminado |
|---|---|---|
| **Se conectó un nuevo dispositivo móvil** | NEW_DEVICE_CONNECTED | 30 días |
| **La lista de perfiles se solicitó correctamente** | PROFILELIST_COMMAND_SUCCESSFULL | 30 días |
| **El perfil se ha instalado correctamente** | INSTALLPROFILE_COMMAND_SUCCESSFULL | 30 días |
| **El perfil se ha eliminado correctamente** | REMOVEPROFILE_COMMAND_SUCCESSFULL | 30 días |
| **La lista de perfiles de aprovisionamiento se solicitó correctamente** | PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL | 30 días |
| **El perfil de aprovisionamiento se ha instalado correctamente** | INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL | 30 días |
| **El perfil de aprovisionamiento se ha eliminado correctamente** | REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL | 30 días |
| **La lista de certificados digitales se solicitó correctamente** | CERTIFICATELIST_COMMAND_SUCCESSFULL | 30 días |
| **La lista de aplicaciones instaladas se solicitó correctamente** | INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL | 30 días |
| **La información general sobre el dispositivo móvil se solicitó correctamente** | DEVICEINFORMATION_COMMAND_SUCCESSFULL | 30 días |
| **La información de seguridad se solicitó correctamente** | SECURITYINFO_COMMAND_SUCCESSFULL | 30 días |
| **El dispositivo móvil se bloqueó correctamente** | DEVICELOCK_COMMAND_SUCCESSFULL | 30 días |
| **La contraseña se restableció correctamente** | CLEARPASSCODE_COMMAND_SUCCESSFULL | 30 días |
| **Los datos del dispositivo móvil se eliminaron correctamente** | ERASEDEVICE_COMMAND_SUCCESSFULL | 30 días |
| **La app se ha instalado correctamente** | INSTALLAPPLICATION_COMMAND_SUCCESSFULL | 30 días |
| **El código de canje se estableció correctamente para la aplicación** | APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL | 30 días |
| **La lista de apps administradas se solicitó correctamente** | MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL | 30 días |
| **La aplicación administrada se eliminó correctamente** | REMOVEAPPLICATION_COMMAND_SUCCESSFULL | 30 días |
| **La configuración de roaming se aplicó correctamente** | SETROAMINGSETTINGS_COMMAND_SUCCESSFUL | 30 días |

## Bloquear eventos frecuentes

Esta sección proporciona información sobre la administración del bloqueo de eventos frecuentes y la eliminación del bloqueo de eventos frecuentes.

## Acerca del bloqueo de eventos frecuentes

Una aplicación administrada, por ejemplo, Kaspersky Endpoint Security para Windows, instalada en uno o varios dispositivos administrados puede enviar muchos eventos del mismo tipo al Servidor de administración. La recepción de eventos frecuentes puede sobrecargar la base de datos del Servidor de administración y sobrescribir otros eventos. El Servidor de administración comienza a bloquear los eventos más frecuentes cuando el número de todos los eventos recibidos supera el límite especificado para la base de datos.

El Servidor de administración bloquea la recepción de los eventos frecuentes automáticamente. No puede bloquear los eventos frecuentes usted mismo, ni elegir qué eventos bloquear.

Si quiere saber si un evento está bloqueado, puede ver la lista de notificaciones o puede verificar si este evento está presente en la sección **Bloqueo de eventos frecuentes** de las propiedades del Servidor de administración. Si el evento está bloqueado, puede hacer lo siguiente:

- Si quiere evitar que se sobrescriba la base de datos, puede seguir bloqueando la recepción de dicho tipo de eventos.
- Por ejemplo, si quiere encontrar el motivo del envío de los eventos frecuentes al Servidor de administración puede desbloquear los eventos frecuentes y seguir recibiendo los eventos de este tipo de todas formas.
- Si quiere seguir recibiendo los eventos frecuentes hasta que se vuelvan a bloquear, puede eliminar el bloqueo de los eventos frecuentes.

## Administrar el bloqueo de eventos frecuentes

El Servidor de administración bloquea la recepción automática de los eventos frecuentes, pero se puede desbloquear y seguir recibiendo los eventos frecuentes. También puede bloquear la recepción de los eventos frecuentes que haya desbloqueado antes.

*Para administrar el bloqueo de eventos frecuentes:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, vaya a la sección **Bloqueo de eventos frecuentes**.

3. En la sección **Bloqueo de eventos frecuentes**:

   - Si desea desbloquear la recepción de eventos frecuentes:

     a. Seleccione los eventos frecuentes que desea desbloquear y, a continuación, haga clic en el botón **Excluir**.

     b. Haga clic en el botón **Guardar**.

   - Si desea bloquear la recepción de eventos frecuentes:

     a. Seleccione los eventos frecuentes que desea bloquear y, a continuación, haga clic en el botón **Bloquear**.

     b. Haga clic en el botón **Guardar**.

El Servidor de administración recibe los eventos frecuentes desbloqueados y no recibe los eventos frecuentes bloqueados.

## Eliminar el bloqueo de eventos frecuentes

Puede eliminar el bloqueo de los eventos frecuentes y empezar a recibirlos hasta que el Servidor de administración vuelva a bloquear estos eventos frecuentes.

*Para eliminar el bloqueo de eventos frecuentes:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, vaya a la sección **Bloqueo de eventos frecuentes**.

3. En la sección **Bloqueo de eventos frecuentes**, seleccione los tipos de eventos frecuentes para los que desea eliminar el bloqueo.

4. Haga clic en el botón **Eliminar del bloqueo**.

El evento frecuente se elimina de la lista de eventos frecuentes. El Servidor de administración recibirá los eventos de este tipo.

## Recepción de eventos de Kaspersky Security for Microsoft Exchange Servers

La información sobre eventos durante el funcionamiento de las aplicaciones administradas, como Kaspersky Endpoint Security para Windows, se transfiere desde los dispositivos administrados y se registra en la base de datos del Servidor de administración. De manera predeterminada, los eventos de Kaspersky Security for Microsoft Exchange Server versión 9.0 MR6 y anteriores no se registran en la base de datos del Servidor de administración. Si Kaspersky Security for Microsoft Exchange Servers versión 9.0 MR6 o anteriores está instalado en los dispositivos administrados de su organización y desea recibir eventos de esta aplicación, habilite el registro de eventos para esta aplicación con la utilidad klscflag.

*Para habilitar el registro de eventos para Kaspersky Security for Microsoft Exchange Servers:*

1. En el dispositivo del Servidor de administración, ejecute el símbolo del sistema de Windows en una cuenta con derechos de administrador.

2. Cambie su directorio actual a la carpeta de instalación de Kaspersky Security Center (generalmente, C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).

3. Ejecute el siguiente comando:

   - Instalación del Servidor de administración en un clúster de conmutación por error de Windows Server:

     ```
     klscflag.exe --stp cluster -fset -pv klserver -n
     KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```

   - En el Servidor de administración instalado en un nodo del clúster de conmutación por error de Kaspersky Security Center:

     ```
     klscflag.exe --stp klfoc -fset -pv klserver -n
     KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```

   - Para el Servidor de administración que no funciona en un clúster:

     ```
     klscflag.exe -fset -pv klserver -n KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d
     -v 0
     ```

El registro de eventos para Kaspersky Security for Microsoft Exchange Servers está habilitado.

Para Kaspersky Security for Microsoft Exchange Servers, no puede establecer el plazo de almacenamiento de los eventos ni seleccionar qué eventos deben guardarse en el repositorio del Servidor de administración. Puede establecer el número máximo de eventos que se pueden guardar en el repositorio. Esta configuración se aplica a los eventos recibidos de todas las aplicaciones de Kaspersky.

# Notificaciones y estados de los dispositivos

En esta sección, encontrará información para ver las notificaciones, configurar el envío de notificaciones, usar los estados de los dispositivos y habilitar los cambios de estado para los dispositivos.

# Uso de notificaciones

Las notificaciones le alertan acerca de eventos y le ayudan a acelerar sus respuestas a estos eventos mediante la realización de acciones recomendadas o acciones que considere apropiadas.

Según el método de la notificación elegido, están disponibles los siguientes tipos de notificaciones:

- Notificaciones en pantalla.
- Notificaciones por SMS.
- Notificaciones por correo electrónico.
- Notificaciones por archivo ejecutable o script.

## Notificaciones en pantalla.

Las notificaciones en pantalla le alertan sobre eventos agrupados por niveles de importancia (*Crítico*, *Advertencia* e *Informativo*).

La notificación en pantalla puede tener uno de estos dos estados:

- *Revisado*. Significa que realizó la acción recomendada para la notificación o que asignó este estado para la notificación manualmente.
- *No revisado*. Significa que no realizó la acción recomendada para la notificación o que asignó este estado para la notificación manualmente.

De forma predeterminada, la lista de notificaciones incluye notificaciones en el estado *No revisado*.

Puede supervisar la red de su organización, ver las notificaciones en pantalla y responder a ellas en tiempo real.

## Notificaciones por correo electrónico, por SMS y por archivo ejecutable o script

Kaspersky Security Center ofrece la capacidad de supervisar la red de su organización enviando notificaciones sobre cualquier evento que considere importante. Para cualquier evento, puede configurar notificaciones por correo electrónico, SMS o ejecutando un archivo ejecutable o un script.

Al recibir notificaciones por correo electrónico o SMS, puede decidir su respuesta a un evento. Esta respuesta debe ser la más adecuada para la red de su organización. Al ejecutar un archivo ejecutable o una secuencia de comandos, predefinirá una respuesta a un evento. También puede considerar ejecutar un archivo ejecutable o una secuencia de comandos como respuesta principal a un evento. Después de que se ejecute el archivo ejecutable, puede seguir otros pasos para responder al evento.

# Visualización de notificaciones en pantalla

Puede ver las notificaciones en pantalla de tres formas:

- En la sección **Supervisión e informes** →**Notificaciones**. Aquí puede ver las notificaciones relacionadas con las categorías predefinidas.
- En una ventana separada que se puede abrir sin importar qué sección esté usando en ese momento. En este caso, puede marcar las notificaciones como revisadas.
- En el widget **Notificaciones por nivel de gravedad seleccionado**, en la sección **Supervisión e informes**→ **Panel**. En el widget, puede ver solo notificaciones de eventos que se encuentran en los niveles de importancia *Crítico* y *Advertencia*.

Puede realizar acciones, por ejemplo, puede responder a un evento.

*Para ver las notificaciones desde las categorías predefinidas:*

1. En el menú principal, vaya a **Supervisión e informes** → **Notificaciones**.

   La categoría **Todas las notificaciones** se selecciona en el panel izquierdo y se muestran todas las notificaciones en el panel derecho.

2. En el panel izquierdo, seleccione una de las categorías:

   - **Despliegue**
   - **Dispositivos**
   - **Protección**
   - **Actualizaciones** (esto incluye notificaciones sobre las aplicaciones de Kaspersky disponibles para descargar y notificaciones sobre las actualizaciones que se han descargado para las bases de datos antivirus)
   - **Prevención de exploits**
   - **Servidor de administración** (esto incluye eventos que conciernen únicamente al Servidor de administración)
   - **Vínculos útiles** (esto incluye enlaces a recursos de Kaspersky, por ejemplo, Servicio de soporte técnico de Kaspersky, foro de Kaspersky, página de renovación de licencia o Enciclopedia de TI de Kaspersky)

   Se muestra una lista de notificaciones de la categoría seleccionada. La lista contiene lo siguientes:

- Ícono relacionado con el tema de la notificación: despliegue (), protección (), actualizaciones (), administración de dispositivos (), prevención de exploits (), servidor de administración ().
- Nivel de importancia de la notificación. Se muestran notificaciones de los siguientes niveles de importancia: **Notificaciones críticas** (), **Notificaciones de advertencia** (), **Notificaciones de información**. Las notificaciones de la lista se agrupan por niveles de importancia.
- **Notificación**. Esto contiene una descripción de la notificación.

- **Acción**. Esto contiene un vínculo a una acción rápida que le recomendamos que realice. Por ejemplo, al hacer clic en este vínculo, puede ir al repositorio e instalar aplicaciones de seguridad en los dispositivos, o ver una lista de dispositivos o una lista de eventos. Después de realizar la acción recomendada para la notificación, a esta notificación se le asigna el estado *Revisado*.

- **Antigüedad del estado** Esto contiene la cantidad de días u horas que han pasado desde el momento en que se registró la notificación en el Servidor de administración.

*Para ver las notificaciones en pantalla en una ventana separada por nivel de importancia:*

1. En la esquina superior derecha de Kaspersky Security Center Web Console, haga clic en el icono del banderín ( ).

   Si el ícono del banderín tiene un punto rojo, hay notificaciones por revisar.

   Se abrirá una ventana con la lista de notificaciones. De forma predeterminada, se selecciona la pestaña **Todas las notificaciones** y se agrupan las notificaciones por nivel de importancia: *Crítico*, *Advertencia* e *Información*.

2. Seleccione la pestaña **Sistema**.

   Se muestra la lista de notificaciones de niveles de importancia *Crítico* ( ) y *Advertencia* ( ). La lista de notificaciones incluye lo siguiente:

   - Marcador de color. Las notificaciones críticas están marcadas en rojo. Las notificaciones de advertencia están marcadas en amarillo.
   - Ícono que indica el tema de la notificación: despliegue ( ), protección ( ), actualizaciones ( ), administración de dispositivos ( ), prevención de exploits ( ), servidor de administración ( ).
   - Descripción de la notificación.
   - Ícono del banderín. El ícono del banderín será de color gris si las notificaciones tienen asignado el estado *No revisado*. Si selecciona el ícono del banderín gris y asigna el estado *Revisado* a una notificación, el ícono cambiará de color al blanco.
   - Enlace a la acción recomendada. Cuando realiza la acción recomendada después de hacer clic en el vínculo, a la notificación se le asigna el estado *Revisado*.
   - Número de días que han pasado desde la fecha en que se registró la notificación en el Servidor de administración.

3. Seleccione la pestaña **Más**.

   Se muestra la lista de notificaciones de nivel de importancia *Información*.

   La organización de la lista es la misma que para la lista en la pestaña **Sistema** (consulte la descripción anterior). La única diferencia es la ausencia de un marcador de color.

Puede filtrar las notificaciones por el intervalo de fecha en que se registraron en el Servidor de administración. Use la casilla **Mostrar filtro** para administrar el filtro.

*Ver notificaciones en pantalla en el widget:*

1. En la sección **Panel**, seleccione **Agregar o restaurar widget web**.

2. En la ventana que se abre, haga clic en la categoría **Otros**, seleccione el widget **Notificaciones por nivel de gravedad seleccionado** y haga clic en Agregar.

   El widget aparece ahora en la pestaña **Panel**. De forma predeterminada, las notificaciones del nivel de importancia *Crítico* se muestran en el widget.

   Puede hacer clic en el botón **Configuración** en el widget y cambiar la configuración del widget para ver las notificaciones del nivel de importancia *Advertencia*. O puede agregar otro widget: **Notificaciones por nivel de gravedad seleccionado**, con un nivel de importancia *Advertencia*.

   La lista de notificaciones en el widget está limitada por su tamaño e incluye dos notificaciones. Estas dos notificaciones se refieren a los últimos eventos.

La lista de notificaciones en el widget incluye lo siguiente:

- Ícono relacionado con el tema de la notificación: despliegue (), protección (), actualizaciones (), administración de dispositivos (), prevención de exploits (), servidor de administración ().

- Descripción de la notificación con un vínculo a la acción recomendada. Cuando realiza la acción recomendada después de hacer clic en el vínculo, a la notificación se le asigna el estado *Revisado*.

- Número de días o número de horas que han pasado desde la fecha en que se registró la notificación en el Servidor de administración.

- Enlace a otras notificaciones. Al hacer clic en este vínculo, se le transfiere a la vista de notificaciones en la sección **Notificaciones** de la sección **Supervisión e informes**.

## Acerca de los estados de los dispositivos

Kaspersky Security Center le asigna un estado a cada dispositivo administrado. El estado asignado depende de que se cumplan las condiciones definidas por el usuario. En algunos casos, al asignar un estado a un dispositivo, Kaspersky Security Center tiene en cuenta el indicador de visibilidad del dispositivo en la red (consulte la tabla a continuación). Por ejemplo, si a un dispositivo administrado se le asigna el estado *Crítico* por cumplirse la condición *Las bases de datos están desactualizadas*, y luego se activa el indicador de visibilidad para ese dispositivo, el estado del dispositivo cambia a *Sin inconvenientes*. Si Kaspersky Security Center no encuentra un dispositivo en la red en un plazo de dos horas, el indicador de visibilidad del dispositivo se establece en *No visible*.

Los estados son los siguientes:

- *Crítico* o *Crítico/Visible*

- *Advertencia* o *Advertencia/Visible*

- *Sin inconvenientes* o *Sin inconvenientes/Visible*

En la siguiente tabla, se enumeran las condiciones predeterminadas que se deben cumplir para que se asignen los estados *Crítico* o *Advertencia* a un dispositivo, con todos los valores posibles.

Condiciones para que se asigne un estado a un dispositivo

| Condición | Descripción de la condición | Valores disponibles |
|---|---|---|
| La aplicación de seguridad no está instalada | El Agente de red está instalado en el dispositivo, pero no hay una aplicación de seguridad instalada. | • Interruptor activado.<br>• Interruptor desactivado. |
| Se detectaron demasiados virus | Una tarea de detección de virus (por ejemplo, la tarea *Análisis antimalware*) detectó en el dispositivo una cantidad de virus superior al valor especificado. | Más de 0. |
| El nivel de protección en tiempo real difiere del nivel establecido por el administrador | El dispositivo es visible en la red, pero el nivel de la protección en tiempo real no se corresponde con el que el administrador configuró (en la condición) para el estado del dispositivo. | • Detenida.<br>• En pausa.<br>• En ejecución. |
| No se ha realizado un análisis antimalware en mucho tiempo | El dispositivo está visible en la red y tiene instalada una aplicación de seguridad, pero la tarea *Análisis antimalware* no se ha ejecutado en el intervalo de tiempo especificado. Esta condición se aplica solo a los dispositivos que se agregaron al menos siete días antes a la base de datos del Servidor de administración. | Más de 1 día. |
| Las bases de datos están desactualizadas | El dispositivo es visible en la red y tiene instalada una aplicación de seguridad, pero sus bases de datos antivirus no se han actualizado en el período de tiempo especificado. Esta condición se aplica solo a los dispositivos que se agregaron al menos un día antes a la base de datos del Servidor de administración. | Más de 1 día. |
| Sin conexión desde hace mucho tiempo | El Agente de red está instalado en el dispositivo, pero el dispositivo está apagado y no se ha conectado a un Servidor de administración durante el período de tiempo especificado. | Más de 1 día. |
| Se han detectado amenazas activas | El número de objetos no procesados en la carpeta **Amenazas activas** supera el valor especificado. | Más de 0 elementos. |
| Se debe reiniciar el dispositivo | El dispositivo es visible en la red, pero una aplicación requiere que el dispositivo se reinicie por más tiempo que el intervalo de tiempo especificado y por una de las razones seleccionadas. | Más de 0 minutos. |
| Hay aplicaciones incompatibles instaladas | El dispositivo es visible en la red, pero, al hacer un inventario de software a través del Agente de red, se detectaron aplicaciones incompatibles instaladas en el dispositivo. | • Interruptor desactivado.<br>• Interruptor activado. |
| Se detectaron vulnerabilidades de software | El dispositivo es visible en la red y tiene instalado el Agente de red, pero la tarea *Buscar vulnerabilidades y actualizaciones requeridas* ha encontrado aplicaciones instaladas en el dispositivo que tienen vulnerabilidades con el nivel de gravedad especificado. | • Crítico.<br>• Alto.<br>• Medio.<br>• Ignorar si la vulnerabilidad no se puede reparar.<br>• Ignorar si hay una actualización asignada para instalarse. |
| Licencia caducada | El dispositivo es visible en la red, pero la licencia ha caducado. | • Interruptor desactivado.<br>• Interruptor activado. |
| La licencia está por caducar | El dispositivo es visible en la red, pero la licencia instalada en el mismo caduca en menos días que el número de días especificado. | Menos de 0 días. |
| La búsqueda de actualizaciones de Windows Update no se ha realizado en mucho tiempo | El dispositivo es visible en la red, pero la tarea *Realizar la sincronización de Windows Update* no se ejecutó durante el intervalo de tiempo especificado. | Más de 1 día. |

| Condición | Descripción de la condición | Valores disponibles |
|---|---|---|
| Estado de cifrado no válido | El Agente de red está instalado en el dispositivo, pero el resultado del cifrado del dispositivo es igual al valor especificado. | • No cumple con la directiva porque el usuario no dio su consentimiento (solo para dispositivos externos).<br>• No cumple con la directiva debido a un error.<br>• Se debe reiniciar el dispositivo al aplicar la directiva.<br>• No se ha especificado una directiva de cifrado.<br>• No compatible.<br>• Al aplicar la directiva. |
| La configuración del dispositivo móvil no cumple con la directiva | Los ajustes del dispositivo móvil no son los que se encontraron en la directiva de Kaspersky Endpoint Security para Android durante el chequeo de reglas de cumplimiento normativo. | • Interruptor desactivado.<br>• Interruptor activado. |
| Problemas de seguridad no procesados detectados | Se han encontrado problemas de seguridad sin procesar en el dispositivo. Los problemas de seguridad se pueden crear manualmente por el administrador o automáticamente por las aplicaciones de Kaspersky administradas que se han instalado en el dispositivo cliente. | • Interruptor desactivado.<br>• Interruptor activado. |
| Estado del dispositivo definido por la aplicación | El estado del dispositivo es definido por la aplicación administrada.<br>Los dispositivos administrados pueden tener un estado determinado por las aplicaciones administradas, independientemente de los parámetros de Kaspersky Security Center. Después de que este estado devuelve uno de los estados definidos por Kaspersky Security Center, el Servidor de administración asigna a un dispositivo administrado el estado más crítico de los devueltos por la aplicación administrada y asignados por el Servidor de administración. Los estados definidos por la administración de aplicaciones tienen descripciones transferidas por las aplicaciones administradas. Puede ver las descripciones en la lista de dispositivos administrados, en la columna **Descripción del estado**. | • Interruptor desactivado.<br>• Interruptor activado. |
| El dispositivo no tiene espacio en el disco | El espacio libre en el disco del dispositivo es inferior al valor especificado o el dispositivo no se pudo sincronizar con el Servidor de administración. Los estados *Crítico* o *Advertencia* cambiarán por el estado *Sin inconvenientes* cuando el dispositivo se sincronice correctamente con el Servidor de administración y el espacio libre en el dispositivo supere o iguale el valor especificado. | Más de 0 MB. |
| El dispositivo ha cambiado a no administrado | Durante el descubrimiento de dispositivos, el dispositivo se reconoció como visible en la red, pero hubo más de tres intentos de sincronizar el dispositivo con el Servidor de administración que terminaron con un error. | • Interruptor desactivado.<br>• Interruptor activado. |
| Protección deshabilitada | El dispositivo es visible en la red, pero la aplicación de seguridad del dispositivo ha estado deshabilitada por un tiempo superior al especificado.<br>En este caso, el estado de la aplicación de seguridad es *detenida* o *error*, y difiere del siguiente: *iniciada*, *en ejecución* o *suspendida*. | Más de 0 minutos. |
| La aplicación de seguridad no está en ejecución | El dispositivo es visible en la red y tiene instalada una aplicación de seguridad, pero esa aplicación no se está ejecutando. | • Interruptor desactivado.<br>• Interruptor activado. |

Kaspersky Security Center permite que usted configure la conmutación automática del estado de un dispositivo en un grupo de administración cuando las condiciones especificadas se cumplen. El estado del dispositivo cliente puede hacerse pasar a *Crítico* o *Advertencia* si se cumplen las condiciones configuradas. Si no se cumplen estas condiciones, el dispositivo cliente toma el estado *Sin inconvenientes*.

Cada estado puede corresponderse con distintos valores de una misma condición. De forma predeterminada, por ejemplo, cuando la condición **Las bases de datos están desactualizadas** tiene el valor **Más de 3 días**, se asigna el estado *Advertencia* al dispositivo cliente; si el valor es **Más de 7 días**, se asigna el estado *Crítico*.

Si actualiza Kaspersky Security Center desde la versión anterior, los valores de la condición **Las bases de datos están desactualizadas** para asignar el estado a *Crítico* o *Advertencia* no cambian.

## Configurar cambios de estado para los dispositivos

Puede cambiar las condiciones bajo las cuales se le asignan los estados *Crítico* o *Advertencia* a un dispositivo.

*Para habilitar el cambio de estado a Crítico para los dispositivos:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Jerarquía de grupos**.
2. En la lista de grupos que se abre, haga clic en el vínculo con el nombre del grupo que contenga los dispositivos para los que desee modificar el cambio de estado.
3. En la ventana de las propiedades que se abre, seleccione la pestaña **Estado del dispositivo**.
4. En el panel izquierdo, seleccione **Crítico**.
5. En el panel derecho, en la sección **Fijar en Crítico si esto se cumple**, habilite la condición bajo la cual el estado de un dispositivo cambiará a *Crítico*.

   Solo podrá modificar los ajustes que no estén bloqueados en la directiva primaria.

6. En la lista, seleccione el botón de opción ubicado junto a la condición.
7. En la esquina superior izquierda de la lista, haga clic en el botón **Editar**.
8. Configure el valor necesario para la condición seleccionada.

   No es posible configurar valores para todas las condiciones.
9. Haga clic en **Aceptar**.

Cuando se cumplan las condiciones especificadas, se asignará el estado *Crítico* al dispositivo administrado.

*Para habilitar el cambio de estado a Advertencia para los dispositivos:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Jerarquía de grupos**.
2. En la lista de grupos que se abre, haga clic en el vínculo con el nombre del grupo que contenga los dispositivos para los que desee modificar el cambio de estado.
3. En la ventana de las propiedades que se abre, seleccione la pestaña **Estado del dispositivo**.
4. En el panel izquierdo, seleccione **Advertencia**.

5. En el panel derecho, en la sección **Fijar en Advertencia si esto se cumple**, habilite la condición que hará que el estado de un dispositivo cambie a *Advertencia*.

   Solo podrá modificar los ajustes que no estén bloqueados en la directiva primaria.

6. En la lista, seleccione el botón de opción ubicado junto a la condición.
7. En la esquina superior izquierda de la lista, haga clic en el botón **Editar**.
8. Configure el valor necesario para la condición seleccionada.

   No es posible configurar valores para todas las condiciones.

9. Haga clic en **Aceptar**.

Cuando se cumplan las condiciones especificadas, se asignará el estado *Advertencia* al dispositivo administrado.

## Configurar el envío de notificaciones

Puede configurar notificaciones sobre eventos que ocurren en Kaspersky Security Center. Según el método de la notificación elegido, están disponibles los siguientes tipos de notificaciones:

- Correo electrónico: Cuando se produce un evento, Kaspersky Security Center envía una notificación a las direcciones de correo electrónico especificadas.
- SMS: Cuando se produce un evento, Kaspersky Security Center envía una notificación a los números de teléfono móvil especificados.
- Archivo ejecutable: cuando ocurre un evento, el archivo ejecutable se ejecuta en el Servidor de administración.

*Para configurar la entrega de notificaciones de eventos que ocurren en Kaspersky Security Center:*

1. En el menú principal, haga clic en el icono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abrirá la ventana de propiedades del Servidor de administración, con la pestaña **General** seleccionada.

2. Haga clic en la sección **Notificación**, y en el panel derecho seleccione la pestaña para el método de notificación que desee:

   - Correo electrónico

La pestaña **Correo electrónico** permite configurar la notificación de eventos por correo electrónico.

En el campo **Direcciones de los destinatarios**, especifique las direcciones de correo electrónico a las que la aplicación enviará notificaciones. Puede especificar varias direcciones en este campo, separándolas con punto y coma.

En el campo **Servidores SMTP**, especifique las direcciones del servidor de correo, separándolas con punto y coma. Puede utilizar los siguientes parámetros:

- Dirección IPv4 o IPv6
- Nombre de la red de Windows (nombre NetBIOS) del dispositivo
- Nombre DNS del servidor SMTP

En el campo **Puerto de los servidores SMTP**, especifique el número de un puerto de comunicación del servidor SMTP. El número de puerto predeterminado es 25.

Si habilita la opción **Usar búsqueda de MX por DNS**, puede utilizar varios registros MX de las direcciones IP para el mismo nombre DNS del servidor SMTP. El mismo nombre DNS puede tener varios registros MX con diferentes valores de prioridad de recepción de mensajes de correo electrónico. El Servidor de administración intenta enviar notificaciones del correo electrónico al servidor SMTP en orden ascendente de prioridad de registros MX.

Si habilita la opción **Usar búsqueda de MX por DNS** y no habilita el uso de la configuración de TLS, le recomendamos que use la configuración de DNSSEC en el dispositivo de su servidor como medida adicional de protección en el envío de notificaciones del correo electrónico.

Si habilita la opción **Utilizar autenticación ESMTP**, puede especificar la configuración de autenticación ESMTP en los campos **Nombre de usuario** y **Contraseña**. De forma predeterminada, la opción está deshabilitada y la configuración de autenticación ESMTP no está disponible.

Puede especificar la configuración de TLS para la conexión con un servidor SMTP:

- **No usar TLS**

Puede seleccionar esta opción si desea deshabilitar el cifrado de mensajes de correo electrónico.

- **Usar TLS si es compatible con el servidor SMTP**

Puede seleccionar esta opción si desea usar una conexión TLS con un servidor SMTP. Si el servidor SMTP no es compatible con TLS, el Servidor de administración se conecta con el servidor SMTP sin usar TLS.

- **Usar siempre TLS, comprobar la validez del certificado del servidor**

Puede seleccionar esta opción si desea usar la configuración de autenticación de TLS. Si el servidor SMTP no es compatible con TLS, el Servidor de administración no puede conectarse al servidor SMTP.

Le recomendamos que use esta opción para una mejor protección de la conexión con un servidor SMTP. Si selecciona esta opción, puede establecer la configuración de autenticación para una conexión TLS.

Si selecciona el valor **Usar siempre TLS, comprobar la validez del certificado del servidor**, puede especificar un certificado para la autenticación del servidor SMTP y elegir si desea habilitar la comunicación a través de cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. También puede especificar un certificado para la autenticación de un cliente en el servidor SMTP.

Puede especificar certificados para una conexión TLS al hacer clic en el enlace **Especificar certificados**:

- Busque un archivo de certificados del servidor SMTP:

Puede recibir un archivo con la lista de certificados de una autoridad de certificación confiable y cargar el archivo al Servidor de administración. Kaspersky Security Center verifica si el certificado de un servidor SMTP también está firmado por una autoridad de certificación confiable. Si el certificado de un servidor SMTP no se recibe de una autoridad de certificación confiable, Kaspersky Security Center no podrá conectarse al servidor SMTP.

- Busque un archivo de certificados cliente:

Puede utilizar un certificado recibido de cualquier fuente (por ejemplo, de una entidad de certificación de confianza). Deberá especificar el certificado y su clave privada. Puede usar, para ello, alguno de los siguientes tipos de certificado:

- Certificado X-509:

Debe especificar un archivo con el certificado y un archivo con la clave privada. Estos dos archivos no dependen el uno del otro y el orden en que se los carga no es importante. Cuando se cargan ambos archivos, debe especificar la contraseña para decodificar la clave privada. Si la clave privada no está codificada, puede dejar la contraseña en blanco.

- Contenedor pkcs12:

Debe cargar un solo archivo que contenga el certificado y la clave privada. Cuando se carga el archivo, debe especificar la contraseña para decodificar la clave privada. Si la clave privada no está codificada, puede dejar la contraseña en blanco.

En el campo **Asunto**, especifique el asunto del correo electrónico. Puede dejar este campo vacío.

En la lista desplegable **Plantilla de asunto**, seleccione la plantilla para su asunto. Una variable determinada por la plantilla seleccionada se coloca automáticamente en el campo **Asunto**. Puede crear un asunto de correo electrónico seleccionando varias plantillas de asunto.

En el campo **Dirección de correo electrónico del remitente**, escriba la dirección de correo electrónico del remitente. Si deja este campo vacío, de forma predeterminada, se utiliza la dirección del destinatario. Se recomienda no utilizar direcciones de correo electrónico falsas.

El campo **Mensaje de notificación** contiene texto estándar con información sobre el evento que la aplicación envía cuando ocurre un evento. Este texto incluye parámetros sustitutos, como el nombre del evento, el nombre del dispositivo y el nombre del dominio. Puede editar el texto del mensaje agregando otros parámetros sustitutos con detalles más relevantes del evento.

> Si el texto de la notificación contiene un signo de porcentaje (%), debe escribirlo dos veces seguidas para permitir el envío de mensajes. Por ejemplo: "La carga de la CPU es 100 %%".

Al hacer clic en el vínculo **Configurar el límite numérico de notificaciones** podrá especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

Al hacer clic en el botón **Enviar mensaje de prueba**, podrá verificar si configuró las notificaciones correctamente: la aplicación envía una notificación de prueba a las direcciones de correo electrónico que especificó.

- SMS

La ficha **SMS** permite configurar la transmisión de notificaciones por SMS de diversos eventos a un teléfono celular. Los mensajes SMS se envían a través de una pasarela de correo.

En el campo **Servidores SMTP**, especifique las direcciones del servidor de correo, separándolas con punto y coma. Puede utilizar los siguientes parámetros:

- Dirección IPv4 o IPv6
- Nombre de la red de Windows (nombre NetBIOS) del dispositivo
- Nombre DNS del servidor SMTP

En el campo **Puerto de los servidores SMTP**, especifique el número de un puerto de comunicación del servidor SMTP. El número de puerto predeterminado es 25.

Si habilita la opción **Utilizar autenticación ESMTP**, puede especificar la configuración de autenticación ESMTP en los campos **Nombre de usuario** y **Contraseña**. De forma predeterminada, la opción está deshabilitada y la configuración de autenticación ESMTP no está disponible.

Puede especificar la configuración de TLS para la conexión con un servidor SMTP:

- **No usar TLS**

Puede seleccionar esta opción si desea deshabilitar el cifrado de mensajes de correo electrónico.

- **Usar TLS si es compatible con el servidor SMTP**

Puede seleccionar esta opción si desea usar una conexión TLS con un servidor SMTP. Si el servidor SMTP no es compatible con TLS, el Servidor de administración se conecta con el servidor SMTP sin usar TLS.

- **Usar siempre TLS, comprobar la validez del certificado del servidor**

Puede seleccionar esta opción si desea usar la configuración de autenticación de TLS. Si el servidor SMTP no es compatible con TLS, el Servidor de administración no puede conectarse al servidor SMTP.

Le recomendamos que use esta opción para una mejor protección de la conexión con un servidor SMTP. Si selecciona esta opción, puede establecer la configuración de autenticación para una conexión TLS.

Si selecciona el valor **Usar siempre TLS, comprobar la validez del certificado del servidor**, puede especificar un certificado para la autenticación del servidor SMTP y elegir si desea habilitar la comunicación a través de cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. También puede especificar un certificado para la autenticación de un cliente en el servidor SMTP.

Puede especificar un archivo de certificado de servidor SMTP al hacer clic en el enlace **Especificar certificados**:

Puede recibir un archivo con la lista de certificados de una autoridad de certificación confiable y cargar el archivo al Servidor de administración. Kaspersky Security Center verifica si el certificado de un servidor SMTP también está firmado por una autoridad de certificación confiable. Si el certificado de un servidor SMTP no se recibe de una autoridad de certificación confiable, Kaspersky Security Center no podrá conectarse al servidor SMTP.

En el campo **Direcciones de los destinatarios**, especifique las direcciones de correo electrónico a las que la aplicación enviará notificaciones. Puede especificar varias direcciones en este campo, separándolas con punto y coma. Las notificaciones se enviarán a los números de teléfono asociados con las direcciones de correo electrónico especificadas.

En el campo **Asunto**, especifique el asunto del correo electrónico.

En la lista desplegable **Plantilla de asunto**, seleccione la plantilla para su asunto. Una variable de acuerdo con la plantilla seleccionada se coloca en el campo **Asunto**. Puede crear un asunto de correo electrónico seleccionando varias plantillas de asunto.

En el campo **Dirección de correo electrónico del remitente: Si deja este campo en blanco, se usará la dirección del destinatario. Advertencia: No se recomienda usar una dirección ficticia**, escriba la dirección de correo electrónico del remitente. Si deja este campo vacío, de forma predeterminada, se utiliza la dirección del destinatario. Se recomienda no utilizar direcciones de correo electrónico falsas.

En el campo **Teléfonos de destinatarios de SMS**, especifique los números de teléfono celular de los destinatarios de notificaciones por SMS.

En el campo **Mensaje de notificación** se especifica un con información sobre el evento que la aplicación envía cuando un evento ocurre. Este texto puede incluir parámetros sustitutos, como el nombre del evento, el nombre del dispositivo y el nombre del dominio.

Si el texto de la notificación contiene un signo de porcentaje (%), debe escribirlo dos veces seguidas para permitir el envío de mensajes. Por ejemplo: "La carga de la CPU es 100 %%".

Haga clic en el vínculo **Configurar el límite numérico de notificaciones** para especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

Haga clic en **Enviar mensaje de prueba** para verificar si configuró las notificaciones correctamente: la aplicación envía una notificación de prueba al destinatario que especificó.

- **Archivo ejecutable para ejecutar**

  Si se selecciona este método de notificación, en el campo de entrada puede especificar la aplicación que se iniciará cuando ocurra un evento.

  En el campo **Archivo ejecutable que se ejecutará en el Servidor de administración cuando ocurra un evento**, escriba el nombre y la carpeta del archivo que se ejecutará. Antes de especificar el archivo, prepare el archivo y especifique los marcadores que definan los detalles del evento que se enviará en el mensaje de notificación. La carpeta y el archivo que especifique deben estar ubicados en el Servidor de administración.

  Al hacer clic en el vínculo **Configurar el límite numérico de notificaciones** podrá especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

3. En la pestaña, defina la configuración de la notificación.

4. Haga clic en el botón **Aceptar** para cerrar la ventana de propiedades del Servidor de administración.

   La configuración de entrega de notificaciones guardada se aplica a todos los eventos que ocurren en Kaspersky Security Center.

Puede anular la configuración de entrega de notificación para ciertos eventos en la sección **Configuración de eventos** de la Configuración del Servidor de administración, de una configuración de directiva o de una configuración de aplicación.

## Notificaciones de eventos que se muestran al ejecutar un archivo ejecutable

Kaspersky Security Center puede notificar al administrador acerca de los eventos en dispositivos cliente al abrir un archivo ejecutable. El archivo ejecutable debe contener otro archivo ejecutable con marcadores del evento que se transmitirá al administrador (consulte la siguiente tabla).

Marcadores para describir un evento

| Marcador | Descripción del marcador |
|---|---|
| %SEVERITY% | Gravedad del evento. Valores posibles:<br>• **Información**<br>• **Advertencia**<br>• **Error**<br>• **Crítico** |
| %COMPUTER% | Nombre del dispositivo en el cual sucedió el evento.<br>La longitud máxima del nombre del dispositivo es de 256 caracteres. |
| %DOMAIN% | Nombre de dominio del dispositivo en el cual sucedió el evento. |
| %EVENT% | Nombre del tipo de evento.<br>La longitud máxima del nombre del tipo de evento es de 50 caracteres. |
| %DESCR% | Descripción del evento.<br>La longitud máxima de la descripción es de 1000 caracteres. |
| %RISE_TIME% | Hora de creación del evento. |
| %KLCSAK_EVENT_TASK_DISPLAY_NAME% | Nombre de la tarea.<br>La longitud máxima del nombre de la tarea es de 100 caracteres. |
| %KL_PRODUCT% | Nombre de la aplicación. |
| %KL_VERSION% | Número de versión de la aplicación. |
| %KLCSAK_EVENT_SEVERITY_NUM% | Número de gravedad del evento. Valores posibles:<br>• 1—**Información**<br>• 2—**Advertencia**<br>• 3—**Error**<br>• 4—**Crítico** |
| %HOST_IP% | Dirección IP del dispositivo en el cual sucedió el evento. |
| %HOST_CONN_IP% | Dirección IP de conexión del dispositivo en el cual sucedió el evento. |

Ejemplo:
Las notificaciones de eventos se envían a través de un archivo ejecutable (como script1.bat) dentro del que se inicia otro archivo ejecutable (como script2.bat) con el marcador %COMPUTER%. Cuando sucede un evento, el archivo script1.bat se ejecuta en el dispositivo del administrador, que a su vez ejecuta el archivo script2.bat con el marcador %COMPUTER%. El administrador luego recibe el nombre del dispositivo en el cual sucedió el evento.

# Novedades de Kaspersky

En esta sección, encontrará información para utilizar, configurar y deshabilitar las novedades de Kaspersky.

## Acerca de las novedades de Kaspersky

La sección de anuncios de Kaspersky (**Supervisión e informes → Anuncios de Kaspersky**) lo mantiene informado al brindarle información relacionada con su versión de Kaspersky Security Center y las aplicaciones administradas instaladas en los dispositivos administrados. Kaspersky Security Center actualiza periódicamente la información de esta sección al eliminar anuncios obsoletos y agregar información nueva.

Kaspersky Security Center muestra solo los anuncios de Kaspersky que se relacionan con el Servidor de administración conectado actualmente y las aplicaciones de Kaspersky instaladas en los dispositivos administrados de este Servidor de administración. Las novedades de cada tipo de Servidor de administración (primario, secundario o virtual) se muestran por separado.

El Servidor de administración debe tener una conexión a Internet para recibir los anuncios de Kaspersky.

Las novedades brindan información de distintas clases:

- Novedades sobre temas de seguridad

  Las novedades sobre seguridad están pensadas para que mantenga actualizadas y en perfectas condiciones de funcionamiento las aplicaciones de Kaspersky instaladas en su red. Estas novedades pueden dar aviso de actualizaciones críticas que se hayan publicado para las aplicaciones de Kaspersky, de soluciones disponibles para las vulnerabilidades detectadas o de formas de solucionar otros problemas en las aplicaciones de Kaspersky. Las novedades sobre seguridad están habilitadas de forma predeterminada. Si no desea recibir estas novedades, deshabilite la función correspondiente.

  Para mostrarle la información que corresponde a la configuración de protección de su red, Kaspersky Security Center envía datos a los servidores en la nube de Kaspersky y recibe solo los anuncios que se relacionan con las aplicaciones de Kaspersky instaladas en su red. El conjunto de datos que se puede enviar a los servidores se describe en el Contrato de licencia de usuario final que acepta al instalar el Servidor de administración de Kaspersky Security Center.

- Novedades con fines publicitarios

  Las novedades con fines publicitarios pueden ser ofertas especiales para las aplicaciones de Kaspersky, anuncios publicitarios o noticias de Kaspersky. Las novedades con fines publicitarios están deshabilitadas de forma predeterminada. Solo recibirá este tipo de novedades si habilita Kaspersky Security Network (KSN). Si desea deshabilitar las novedades con fines publicitarios, deshabilite KSN.

  Para mostrarle solo información relevante que pueda ser útil para proteger sus dispositivos de red y en sus tareas diarias, Kaspersky Security Center envía datos a los servidores en la nube de Kaspersky y recibe los anuncios correspondientes. Encontrará una descripción de los datos que se pueden transmitir a los servidores en la sección "Datos procesados" de la Declaración de KSN.

La nueva información se divide en las siguientes categorías, según su importancia:

1. Información crítica
2. Noticias importantes
3. Advertencia
4. Información

Cuando aparece nueva información en la sección de novedades de Kaspersky, Kaspersky Security Center Web Console muestra una etiqueta de notificación correspondiente al nivel de importancia de la novedad. Haga clic en la etiqueta para ver la información en la sección de novedades de Kaspersky.

Puede especificar la configuración de los anuncios de Kaspersky, incluidas las categorías de anuncios que desea ver y dónde mostrar la etiqueta de notificación.

# Especificar la configuración de los anuncios de Kaspersky

En la sección Anuncios de Kaspersky, puede especificar la configuración de los anuncios de Kaspersky, incluidas las categorías de anuncios que desea ver y dónde mostrar la etiqueta de notificación.

*Para configurar los anuncios de Kaspersky:*

1. En el menú principal, vaya a **Supervisión e informes** → **Novedades de Kaspersky**.
2. Haga clic en el vínculo **Configuración**.

   Se abre la ventana de configuración de los anuncios de Kaspersky.
3. Configure los siguientes ajustes:

   - Seleccione el nivel de importancia de los anuncios que desea ver. No se mostrarán los anuncios de otras categorías.
   - Seleccione dónde desea ver la etiqueta de notificación. La etiqueta puede aparecer en todas las secciones de la consola o en la sección **Supervisión e informes** y sus subsecciones.
4. Haga clic en el botón **Aceptar**.

   Se especifica la configuración de los anuncios de Kaspersky.

# Dejar de recibir las novedades de Kaspersky

La sección de anuncios de Kaspersky (**Supervisión e informes** → **Anuncios de Kaspersky**) lo mantiene informado al brindarle información relacionada con su versión de Kaspersky Security Center y las aplicaciones administradas instaladas en los dispositivos administrados. Si ya no desea recibir novedades de Kaspersky, puede deshabilitar esta función.

Kaspersky publica dos clases de novedades: novedades sobre temas de seguridad y novedades con fines publicitarios. Puede deshabilitar cada clase de novedad por separado.

*Para dejar de recibir novedades sobre temas de seguridad:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.
2. En la pestaña **General**, vaya a la sección **Novedades de Kaspersky**.
3. Ponga el interruptor en la posición **Novedades sobre seguridad Deshabilitado**.
4. Haga clic en el botón **Guardar**.

   Ya no recibirá novedades de Kaspersky.

Las novedades con fines publicitarios están deshabilitadas de forma predeterminada. Solo recibirá este tipo de novedades si ha habilitado Kaspersky Security Network (KSN). Si quiere deshabilitar las novedades con fines publicitarios, deshabilite KSN.

*Para dejar de recibir novedades que tengan fines publicitarios:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Configuración del proxy de KSN**.

3. Deshabilite la opción **Usar Kaspersky Security Network Habilitado**.

4. Haga clic en el botón **Guardar**.

   Ya no recibirá novedades con fines publicitarios.

# Ver información sobre la detección de amenazas

Puede indicar si desea que la aplicación muestre u oculte información sobre las alertas.

*Para indicar si se deberá mostrar la sección **Alertas** en el menú principal:*

1. En el menú principal, vaya a la configuración de su cuenta y, a continuación, seleccione **Opciones de interfaz.**

2. En la ventana **Opciones de interfaz** que se abre, habilite o deshabilite la opción **Mostrar alertas EDR**.

3. Haga clic en **Guardar**.

La consola muestra la subsección **Alertas** en la sección **Supervisión e informes** del menú principal. En la subsección **Alertas**, podrá ver información sobre la detección de amenazas en los endpoints. Si se agrega una clave de licencia para EDR Optimum, luego Kaspersky Security Center Web Console muestra automáticamente la subsección **Alertas** en la sección **Supervisión e informes** del menú principal. Si lo prefiere, también puede agregar un widget que muestre información sobre las alertas.

> La subsección **Alertas** se muestra automáticamente solo si agregó la clave de licencia para EDR Optimum antes de activar la opción **Mostrar alertas EDR**. Si agregó la clave de licencia después de habilitar la opción **Mostrar alertas EDR**, la subsección **Alertas** se mostrará solo después de que vuelva a activar esta opción.

Para que la tarjeta de alerta muestre correctamente la información detallada sobre las amenazas detectadas, se debe instalar el complemento de Kaspersky Endpoint Agent y la versión compatible del complemento de Kaspersky Endpoint Security (Kaspersky Endpoint Security for Linux 12.1 o posterior, Kaspersky Endpoint Security for Mac 12.1 o posterior, o Kaspersky Endpoint Security para Windows 12.6 o posterior).

Utilice el menú **Filtro** para filtrar las alertas por fecha y valores de campo.

El campo **Tipo de objeto** contiene los siguientes valores:

- Desconocido
- Vínculo de phishing
- Virus
- Troyano

- Herramienta maliciosa
- Puerta trasera
- Gusano
- Otra aplicación
- Adware
- Software pornográfico
- Programa empaquetado peligroso
- Comportamiento peligroso

El campo **Respuesta automática** contiene los siguientes valores:

- Se detectó un objeto malicioso
- Objeto eliminado
- Objeto desinfectado
- El objeto no pudo ser desinfectado
- Objeto puesto en cuarentena
- Archivo protegido por contraseña detectado
- Virus detectados

# Cloud Discovery

Kaspersky Security Center le permite supervisar el uso de los servicios en la nube en dispositivos administrados con Windows y bloquear el acceso a los servicios en la nube que considera no deseados. Cloud Discovery monitorea los intentos de los usuarios de acceder a estos servicios desde navegadores y aplicaciones de escritorio. También supervisa los intentos de los usuarios de acceder a servicios en la nube mediante conexiones no cifradas (por ejemplo, a través del protocolo HTTP). La función permite detectar y detener el uso de servicios en la nube por parte de la llamada "TI invisible".

La capacidad de bloqueo solo está disponible si activó Kaspersky Security Center con una licencia EDR Optimum o XDR Expert de Kaspersky Security Center.

La capacidad de bloqueo solo estará disponible si utiliza Kaspersky Endpoint Security para Windows 11.2 o una versión posterior. Las versiones anteriores de la aplicación de seguridad solo permiten supervisar el uso de servicios en la nube.

Puede habilitar la función Cloud Discovery y seleccionar las directivas o los perfiles de seguridad para los que desee habilitar la función. También puede habilitar o deshabilitar la función para cada directiva o perfil de seguridad de forma independiente. Puede bloquear el acceso a los servicios en la nube a los que no desee que accedan los usuarios.

Para poder bloquear el acceso a servicios en la nube no deseados, asegúrese de que se cumplan los siguientes requisitos previos:

- Utiliza Kaspersky Endpoint Security 11.2 para Windows o una versión posterior. Las versiones anteriores de la aplicación de seguridad solo permiten supervisar el uso de servicios en la nube.
- Compró una licencia del nivel de Kaspersky Next que incluye la posibilidad de bloquear el acceso a servicios en la nube no deseados. Para obtener más información, consulte la Ayuda de Kaspersky Next.

El widget de Cloud Discovery y los informes de Cloud Discovery muestran información sobre los intentos concretados y bloqueados de acceder a servicios en la nube. El widget también muestra el nivel de riesgo de cada servicio en la nube. Kaspersky Security Center obtiene información sobre el uso de los servicios en la nube de todos los dispositivos administrados que están protegidos solo con las directivas o los perfiles de seguridad que tienen la función habilitada.

## Habilitar Cloud Discovery mediante el widget

La función Cloud Discovery permite obtener información sobre el uso de servicios en la nube de todos los dispositivos administrados que se han protegido con directivas de seguridad que tengan la función habilitada. Puede habilitar o deshabilitar Cloud Discovery exclusivamente para la directiva de Kaspersky Endpoint Security para Windows.

Existen dos formas de habilitar la función Cloud Discovery:

- utilizar el widget de Cloud Discovery;
- modificar las propiedades de la directiva de Kaspersky Endpoint Security para Windows.

  Para obtener información detallada sobre cómo habilitar la función Cloud Discovery en las propiedades de la directiva de Kaspersky Endpoint Security para Windows, consulte la sección Cloud Discovery en la Ayuda de Kaspersky Endpoint Security para Windows.

Tenga en cuenta que la función Cloud Discovery solo se puede deshabilitar en los ajustes de la directiva de Kaspersky Endpoint Security para Windows.

Para habilitar Cloud Discovery, debe tener el derecho **Modificar** en el área funcional **Características generales: funcionalidad básica**.

*Para habilitar la función Cloud Discovery mediante el widget:*

1. Vaya a Kaspersky Security Center.
2. En el menú principal, vaya a **Supervisión e informes** → **Panel**.

3. En el widget de **Cloud Discovery**, haga clic en el botón **Habilitar**.

   Si tiene instalada la versión 12.4 de Kaspersky Endpoint Security para Windows, habilite la función Cloud Discovery en las propiedades de la directiva de Kaspersky Endpoint Security para Windows. Para obtener más información, consulte la sección Cloud Discovery de la Ayuda de Kaspersky Endpoint Security para Windows.

   Si su versión de Kaspersky Endpoint Security para Windows es anterior a la 12.4, actualice el complemento de Kaspersky Endpoint Security para Windows a la versión 12.5.

4. En la ventana **Habilitar Cloud Discovery** que se abre, seleccione las directivas de seguridad para las que desea habilitar la función y, luego, haga clic en el botón **Habilitar**.

   Los siguientes ajustes de la directiva se habilitarán automáticamente: **Inyectar script en el tráfico web para interactuar con las páginas web**, **Monitor de sesión web** y **Análisis de conexiones cifradas**.

La función Cloud Discovery queda habilitada y el widget se agrega al panel.

## Agregar el widget de Cloud Discovery al panel

Puede agregar el widget de **Cloud Discovery** al panel para supervisar el uso de servicios en la nube en los dispositivos administrados.

Para agregar el widget de Cloud Discovery al panel, debe tener el derecho **Modificar** en el área funcional **Características generales: Funcionalidad básica**.

*Para agregar el widget de Cloud Discovery al panel:*

1. Vaya a Kaspersky Security Center.
2. En el menú principal, vaya a **Supervisión e informes** → **Panel**.
3. Haga clic en el botón **Agregar o restaurar widget web**.
4. En la lista de widgets disponibles, haga clic en el ícono del corchete angular (>) ubicado junto a la categoría **Otro**.
5. Seleccione el widget **Cloud Discovery** y, luego, haga clic en el botón **Agregar**.

   Si la función Cloud Discovery está deshabilitada, siga las instrucciones en la sección "Habilitar Cloud Discovery mediante el widget".

El widget seleccionado se agrega al final del panel.

## Ver información sobre el uso de servicios en la nube

Puede ver el widget de **Cloud Discovery**, que muestra información sobre los intentos de acceso a servicios en la nube. El widget también muestra el nivel de riesgo de cada servicio en la nube. Kaspersky Security Center obtiene información sobre el uso de los servicios en la nube de todos los dispositivos administrados que están protegidos solo con los perfiles de seguridad que tienen la función habilitada.

Antes de acceder a la información, asegúrese de que se cumplan los siguientes requisitos:

- Que el widget de Cloud Discovery se haya agregado al panel.
- Que la función Cloud Discovery esté habilitada.
- Que tenga el derecho de **Leer** en el área funcional **Características generales: funcionalidad básica**.

*Para ver el widget de Cloud Discovery:*

1. Vaya a Kaspersky Security Center.
2. En el menú principal, vaya a **Supervisión e informes** → **Panel**.

   El widget de **Cloud Discovery** se muestra en el panel.
3. En el lado izquierdo del widget de **Cloud Discovery**, seleccione una categoría de servicios en la nube.

   En la tabla ubicada en el lado derecho del widget, se mostrarán hasta cinco servicios de la categoría seleccionada a los que los usuarios intenten acceder con mayor frecuencia. Se cuentan tanto los intentos exitosos como los bloqueados.
4. En el lado derecho del widget, seleccione un servicio específico.

   En la tabla que verá a continuación, se mostrarán los diez dispositivos que hayan intentado acceder a un servicio con mayor frecuencia. Puede usar esta tabla para generar dos tipos de informes: un informe sobre los intentos de acceso exitosos y un informe sobre los intentos de acceso bloqueados.

   Además, en esta tabla puede bloquear el acceso a un servicio en la nube para un dispositivo específico.

El widget mostrará la información solicitada.

En el widget que se abre, puede hacer lo siguiente:

- dirigirse a la sección **Supervisión e informes** → **Informes** para ver los informes de Cloud Discovery;
- bloquear o permitir el acceso a un servicio de nube seleccionado.

La capacidad de bloqueo solo está disponible si activó Kaspersky Security Center con una licencia EDR Optimum o XDR Expert de Kaspersky Security Center.

La capacidad de bloqueo solo estará disponible si utiliza Kaspersky Endpoint Security para Windows 11.2 o una versión posterior. Las versiones anteriores de la aplicación de seguridad solo permiten supervisar el uso de servicios en la nube.

## Nivel de riesgo de un servicio en la nube

Cloud Discovery indica un nivel de riesgo para cada servicio en la nube. El nivel de riesgo ayuda a determinar qué servicios no se ajustan a los requisitos de seguridad de la organización. Posiblemente quiera tener en cuenta el nivel de riesgo a la hora de decidir si bloqueará el acceso a un determinado servicio.

El nivel de riesgo es un índice estimado; no indica la calidad de un servicio en la nube o del proveedor del servicio. El nivel de riesgo es simplemente una recomendación de los expertos de Kaspersky.

Los niveles de riesgo de los servicios en la nube se muestran en el widget de Cloud Discovery y en la lista de todos los servicios en la nube supervisados.

## Bloquear el acceso a servicios en la nube no deseados

Puede bloquear el acceso a los servicios en la nube a los que no desee que accedan los usuarios. También puede permitir el acceso a servicios en la nube que se encuentren bloqueados.

Al decidir si bloqueará el acceso a un servicio determinado, entre otras consideraciones, es posible que desee tener en cuenta el nivel de riesgo.

El acceso a los servicios en la nube puede bloquearse o permitirse en una directiva o en un perfil de seguridad.

Existen dos formas de bloquear el acceso a servicios en la nube no deseados:

- Utilizar el widget de Cloud Discovery.

  Si elige esta opción, puede bloquear el acceso a servicios individuales.

- Modificar las propiedades de la directiva de Kaspersky Endpoint Security para Windows.

  Si elige esta opción, puede bloquear el acceso a servicios individuales o incluso a categorías completas.

  Para obtener información detallada sobre cómo habilitar la función Cloud Discovery en las propiedades de la directiva de Kaspersky Endpoint Security para Windows, consulte la sección Cloud Discovery en la Ayuda de Kaspersky Endpoint Security para Windows.

*Para bloquear o permitir el acceso a un servicio en la nube mediante el widget:*

1. Abra el widget de Cloud Discovery y seleccione el servicio en la nube en cuestión.
2. En el panel **Los 10 principales dispositivos que utilizan el servicio**, busque la directiva o el perfil de seguridad en que desee bloquear o permitir el servicio.
3. En la línea correspondiente, en la columna **Estado del acceso en la directiva o el perfil**, realice una de las siguientes acciones:
   - Para bloquear el servicio, seleccione **Bloqueado** en la lista desplegable.
   - Para permitir el servicio, seleccione **Permitido** en la lista desplegable.
4. Haga clic en el botón **Guardar**.

El acceso al servicio seleccionado queda bloqueado o permitido en la directiva o el perfil de seguridad.

# Registro de actividad de Kaspersky Security Center Web Console

El registro de actividad de Kaspersky Security Center Web Console puede ayudar a investigar las causas de un mal funcionamiento del software. Cuando se comunique con el Servicio de Soporte técnico de Kaspersky por un mal funcionamiento de Kaspersky Security Center Web Console, los especialistas del Servicio de Soporte técnico de Kaspersky pueden solicitarle los archivos de registro de Kaspersky Security Center Web Console. Los archivos de registro de Kaspersky Security Center Web Console se almacenan en la <carpeta de instalación de Kaspersky Security Center Web Console>/registros durante todo el tiempo que use la aplicación. Los archivos de registro no se envían a los especialistas del Soporte técnico de Kaspersky automáticamente.

*Para activar el registro de actividad de Kaspersky Security Center Web Console,*

Seleccione la casilla **Registrar las actividades de Kaspersky Security Center Web Console**, en la ventana **Configuración de conexión de Kaspersky Security Center Web Console** del Asistente de instalación de Kaspersky Security Center Web Console.

Los archivos de registro están en formato de texto.

Los nombres de los archivos de registro tienen el formato logs- <nombre del componente>.<nombre del dispositivo>-<número de revisión del archivo> .AAAA-MM-DD, donde:

- <nombre del componente> es el nombre del componente Kaspersky Security Center o es el nombre del complemento de administración de Kaspersky Security Center Web Console.
- <nombre de dispositivo> es el nombre del dispositivo en el que se está ejecutando el <nombre de componente>.
- <número de revisión del archivo> es el número del archivo de registro creado para el <nombre del componente> que está en operación en el <nombre del dispositivo>. En un día, se pueden crear varios archivos de registro para el mismo <nombre de componente> y <nombre de dispositivo>. El tamaño máximo de un archivo de registro es de 50 megabytes (MB). Cuando se alcanza el tamaño máximo de archivo, se crea un archivo de registro nuevo. Un archivo de registro nuevo <número de revisión de archivo> se incrementa en 1.
- AAAA, MM y DD son el año, mes y día en que se creó el registro por primera vez. Cuando comienza un día nuevo, se crea un nuevo archivo de registro.

# Integración entre Kaspersky Security Center y otras soluciones

Esta sección describe cómo configurar el acceso desde Kaspersky Security Center Web Console a otra aplicación de Kaspersky, como Kaspersky Managed Detection and Response. Asimismo, esta sección describe cómo configurar la exportación a sistemas SIEM.

# Establecer una conexión en segundo plano

Para permitir que Kaspersky Security Center Web Console realice sus tareas en segundo plano, debe establecer una conexión en segundo plano entre Kaspersky Security Center Web Console y el Servidor de administración. Podrá establecer esta conexión solo si su cuenta tiene el derecho **Modificar ACL de objeto** del área funcional **Características generales: Permisos de usuario**.

Si instala el complemento de Kaspersky Endpoint Security para Windows 12.6 o si actualiza el complemento de Kaspersky Endpoint Security para Windows desde la versión anterior a la 11.7, y aún no se estableció una conexión en segundo plano, se mostrará una notificación que indica que tiene que establecer una conexión en segundo plano. Además, deberá otorgar a la cuenta de servicio los derechos del área funcional **Características generales: Operaciones en el servidor de administración**.

*Para establecer una conexión en segundo plano:*

1. En el menú principal, vaya a **Configuración** → **Integración**.
2. En la sección **Integración**, desplace el botón de alternancia de **Conexión en segundo plano para la integración Habilitada** a la posición HABILITADO para establecer una conexión en segundo plano.
3. En la sección **Habilitar una conexión en segundo plano** abierta, haga clic en el botón **Aceptar**.

Se establece la conexión en segundo plano entre Kaspersky Security Center Web Console y el Servidor de administración. El Servidor de administración crea una cuenta para la conexión en segundo plano y esta cuenta se utiliza como cuenta de servicio para mantener la interacción entre Kaspersky Security Center y otra aplicación o solución de Kaspersky. El nombre de esta cuenta de servicio contiene el prefijo NWCSvcUser.

Por seguridad, el Servidor de administración cambia la contraseña de la cuenta del servicio automáticamente cada 30 días. No puede eliminar la cuenta del servicio manualmente. El Servidor de administración elimina esta cuenta automáticamente si se deshabilita la conexión entre servicios. El Servidor de administración crea una única cuenta de servicio para cada Consola de administración y asigna todas las cuentas de servicio al grupo de seguridad con el nombre ServiceNwcGroup. El Servidor de administración crea automáticamente este grupo de seguridad durante el proceso de instalación de Kaspersky Security Center. No puede eliminar este grupo de seguridad manualmente.

# Exportación de eventos a sistemas SIEM

En esta sección, se brindan instrucciones para configurar la exportación de eventos a un sistema SIEM.

## Configurar la exportación de eventos a sistemas SIEM

Kaspersky Security Center permite la configuración mediante uno de los siguientes métodos: exportar a cualquier sistema SIEM que utilice formato Syslog, exportar a los sistemas SIEM QRadar, Splunk y ArcSight que utilizan formatos LEEF y CEF o exportar eventos a sistemas SIEM directamente desde la base de datos de Kaspersky Security Center. Cuando complete este escenario, el Servidor de administración enviará los eventos al sistema SIEM automáticamente.

### Requisitos previos

Antes de configurar la exportación de eventos en Kaspersky Security Center, haga lo siguiente:

- Lea sobre los métodos disponibles para exportar eventos.
- Asegúrese de contar con los valores de la configuración del sistema.

Los pasos aquí descritos pueden realizarse en cualquier orden.

El proceso para exportar eventos a un sistema SIEM consiste de los siguientes pasos:

- **Configuración del sistema SIEM para que reciba eventos de Kaspersky Security Center**

  Instrucciones: Configurar la exportación de eventos en un sistema SIEM

- **Seleccionar eventos que desea exportar al sistema SIEM:**

  Instrucciones:

  - Consola de administración: Marcar eventos de una aplicación de Kaspersky para exportarlos en formato Syslog, Marcar eventos generales para que se los exporte en formato Syslog
  - Kaspersky Security Center Web Console: Marcar eventos de una aplicación de Kaspersky para que se los exporte en formato Syslog, Marcar eventos generales para que se los exporte en formato Syslog

- **Configuración de la exportación de eventos a sistemas SIEM mediante uno de los siguientes métodos:**

  - Mediante los protocolos TCP/IP, UDP o TLS sobre TCP

    Instrucciones:

    - Consola de administración: Configurar la exportación de eventos a sistemas SIEM
    - Kaspersky Security Center Web Console: Configurar la exportación de eventos a sistemas SIEM

  - Exporte los eventos directamente desde la base de datos de Kaspersky Security Center (la base de datos de Kaspersky Security Center proporciona un conjunto de vistas públicas, que se describen en el documento klakdb.chm).

### Resultados

Tras configurar la exportación de eventos al sistema SIEM, si marcó eventos como exportables, podrá ver los resultados de la exportación.

## Antes de comenzar

Al configurar la exportación automática de eventos en Kaspersky Security Center, debe especificar algunas de las configuraciones del sistema SIEM. Se recomienda que verifique estas configuraciones de antemano a fin de prepararse para configurar Kaspersky Security Center.

Para configurar correctamente el envío automático de eventos a un sistema SIEM, debe conocer los valores de los siguientes parámetros:

- **Dirección del servidor del sistema SIEM**

  La dirección IP del servidor en el que está instalado el sistema SIEM. Encontrará este valor en la configuración del sistema SIEM.

- **Puerto del servidor del sistema SIEM**

  El número de puerto usado para establecer una conexión entre Kaspersky Security Center y su servidor del sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center y en la configuración del destinatario de su sistema SIEM.

- **Protocolo**

  Protocolo usado para transferir mensajes de Kaspersky Security Center a su sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center y en la configuración del destinatario de su sistema SIEM.

# Acerca de los eventos en Kaspersky Security Center

Kaspersky Security Center le permite recibir información sobre los eventos de funcionamiento del Servidor de administración y aplicaciones de Kaspersky instaladas en dispositivos administrados. La información sobre estos eventos se guarda en la base de datos del Servidor de administración. Puede exportar esta información a un sistema SIEM externo. Al hacerlo, permitirá que los administradores del sistema SIEM respondan oportunamente a los sucesos del sistema de seguridad que se registren en dispositivos o grupos de dispositivos administrados.

## Tipos de evento

En Kaspersky Security Center existen los siguientes tipos de eventos:

- Eventos generales. Esta clase de evento ocurre en todas las aplicaciones de Kaspersky administradas. Un ejemplo de evento general es Brote de virus. Los eventos generales tienen una sintaxis y una semántica estrictamente definidas. Los eventos generales se utilizan en, por ejemplo, los paneles e informes.

- Eventos específicos de las aplicaciones de Kaspersky administradas. Cada aplicación de Kaspersky administrada tiene su propio conjunto de eventos.

### Orígenes de eventos

Los eventos pueden ser generados por las siguientes aplicaciones:

- Componentes de Kaspersky Security Center:
  - Servidor de administración
  - Agente de red
  - Servidor de MDM para iOS
- Aplicaciones administradas por Kaspersky

  Para obtener detalles sobre los eventos generados por las aplicaciones administradas por Kaspersky, consulte la documentación de la aplicación correspondiente.

Puede ver la lista completa de los eventos que puede generar una aplicación en la pestaña **Configuración de eventos** en la directiva de la aplicación. Para el Servidor de administración, también puede ver la lista de eventos en las propiedades del Servidor de administración.

### Nivel de importancia de los eventos

Cada evento tiene su propio nivel de importancia. El nivel de importancia que se le asigna a un evento puede variar según las circunstancias en las que ocurre. Existen cuatro niveles de importancia:

- Un *evento crítico* es un evento que se registra cuando ocurre un problema de extrema gravedad, que puede derivar en pérdidas de información, en un error crítico o en un fallo de funcionamiento.
- Un *error funcional* es un evento que se registra cuando ocurre un problema, fallo o error graves en el funcionamiento de la aplicación o en la ejecución de un procedimiento.
- Una *advertencia* es un evento que no necesariamente es grave, pero que anticipa un posible problema en el futuro. La mayoría de los eventos se catalogan como advertencias si, a pesar de que el evento haya ocurrido, la aplicación puede recuperarse sin sufrir una pérdida de información o de funcionalidad.
- Un evento *informativo* es un evento que se registra para informar que una operación o procedimiento se completaron sin errores o que la aplicación funciona correctamente.

Cada evento tiene un plazo de almacenamiento definido, durante el cual lo puede ver o modificar en Kaspersky Security Center. Algunos eventos no se guardan en la base de datos del Servidor de administración de forma predeterminada porque su plazo de almacenamiento está definido en cero. Para que un evento pueda exportarse, debe permanecer almacenado al menos un día en la base de datos del Servidor de administración.

## Acerca de la exportación de eventos

La exportación de eventos puede utilizarse en sistemas centralizados que permiten atender a los problemas de seguridad en un nivel organizativo y técnico. Estos sistemas, denominados sistemas SIEM, brindan servicios para hacer un monitoreo de la seguridad y son capaces de integrar la información de distintas soluciones. Pueden analizar, en tiempo real, los eventos y las alertas de seguridad que generan las aplicaciones, el hardware de red y los centros de operaciones de seguridad (SOC).

Los sistemas SIEM reciben información de muchas fuentes, como redes, soluciones de seguridad, servidores, aplicaciones y bases de datos. Pueden integrar los datos que obtienen para reducir las probabilidades de que un evento crítico pase desapercibido. También pueden realizar análisis automatizados de alertas y eventos correlacionados para notificar a los administradores de cualquier problema de seguridad inmediato. Las alertas de estos sistemas se pueden comunicar a través de un panel o tablero, o se pueden enviar por correo electrónico u otra vía provista por un tercero.

El proceso de exportación de eventos desde Kaspersky Security Center a sistemas SIEM externos involucra a dos partes: un remitente de eventos (Kaspersky Security Center) y un destinatario para los eventos (el sistema SIEM). Para exportar eventos correctamente, debe configurar estos parámetros en su sistema de SIEM y en la Consola de administración de Kaspersky Security Center. No importa cuál de los dos lados se configura primero. Puede configurar la transmisión de eventos en Kaspersky Security Center y luego configurar la recepción de estos por el sistema SIEM, o viceversa.

## Métodos para enviar eventos desde Kaspersky Security Center

Hay tres métodos para enviar eventos desde Kaspersky Security Center a los sistemas externos:

- El envío de eventos a través del protocolo de Syslog a cualquier sistema SIEM

  Usando el protocolo de Syslog, puede transmitir cualquier evento que ocurra en el Servidor de administración de Kaspersky Security Center y en Aplicaciones de Kaspersky instaladas en dispositivos administrados. El protocolo de Syslog es un protocolo de registro de mensajes estándares. Puede utilizarlo para exportar eventos a cualquier sistema SIEM.

  Para ello, debe marcar los eventos que desea transmitir al sistema SIEM. Puede marcar los eventos en Consola de administración o en Kaspersky Security Center Web Console. Solo los eventos marcados se transmitirán al sistema SIEM. Si no marcó nada, no se transmitirá ningún evento.

- Envío de eventos a través de los protocolos CEF y LEEF a sistemas de QRadar, Splunk y ArcSight

  Puede utilizar los protocolos CEF y LEEF para exportar eventos generales. Al exportar eventos a través de los protocolos CEF y LEEF, no tiene la posibilidad de seleccionar eventos específicos para exportarlos. En su lugar, se exportan todos los eventos generales. Para convertir eventos de Kaspersky Security Center a eventos en formato CEF y LEEF, debe utilizar el archivo siem_conversion_rules.xml. Este archivo contiene la lista de atributos de eventos de Kaspersky Security Center y los atributos correspondientes de eventos en formato CEF y LEEF. Además, el archivo siem_conversion_rules.xml contiene las reglas para generar mensajes correspondientes a eventos. Este archivo está incluido en el kit de distribución de Kaspersky Security Center.

  A diferencia del protocolo Syslog, los protocolos CEF y LEEF no son universales. CEF y LEEF están diseñados para los sistemas SIEM apropiados (QRadar, Splunk y ArcSight). Por lo tanto, cuando elige exportar eventos sobre uno de estos protocolos, usa el analizador requerido en el sistema SIEM.

- Directamente desde la base de datos de Kaspersky Security Center a cualquier sistema SIEM

  Este método de exportar eventos puede utilizarse para recibir eventos directamente de vistas públicas de la base de datos mediante consultas de SQL. Los resultados de una pregunta se guardan en un archivo de XML que se puede utilizar como datos de entrada para un sistema externo. Solo los eventos disponibles en vistas públicas se pueden exportar directamente desde la base de datos.

## Recepción de eventos por parte del sistema SIEM

El sistema SIEM debe recibir y correctamente analizar eventos recibidos de Kaspersky Security Center. Para que esto ocurra, el sistema SIEM debe estar correctamente configurado. El proceso de configuración depende del sistema SIEM que se utilice. Sin embargo, existen algunos pasos de configuración generales (como la configuración del receptor y el analizador) que son comunes a todos.

# Acerca de la configuración de la exportación de eventos en un sistema SIEM

El proceso de exportación de eventos desde Kaspersky Security Center a sistemas SIEM externos involucra a dos partes: un remitente de eventos (Kaspersky Security Center) y un destinatario para los eventos (el sistema SIEM). Debe configurar la exportación de eventos en su sistema SIEM y en Kaspersky Security Center.

Los ajustes que especifique en el sistema SIEM dependerán del sistema particular que esté utilizando. En general, para todo sistema SIEM, deberá configurar un receptor y, opcionalmente, un analizador que procese los eventos recibidos.

## Configuración del receptor

Para recibir eventos enviados por Kaspersky Security Center, debe configurar el destinatario en su sistema SIEM. Por lo general, deberá especificar los valores de los siguientes parámetros dentro del sistema SIEM:

- **Protocolo de exportación o tipo de entrada**

  Es el protocolo de transferencia de mensajes, por ejemplo, UDP. Este protocolo debe ser igual que el protocolo que especificó en Kaspersky Security Center.

- **Puerto**

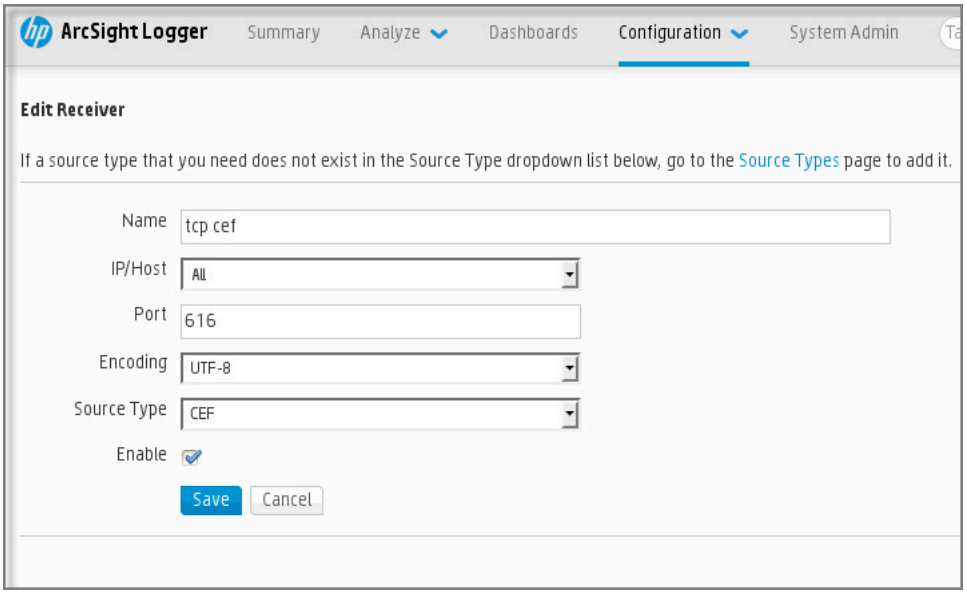
  Número de puerto utilizado para conectarse a Kaspersky Security Center. Este puerto debe ser igual que el puerto que especificó en Kaspersky Security Center.

- **Protocolo de mensajes o tipo de origen**

  El protocolo usado para exportar eventos al sistema SIEM. Puede ser uno de los protocolos estándares: Syslog, CEF o LEEF. El sistema SIEM selecciona el analizador sintáctico del mensaje según el protocolo que especifica.

Según el sistema SIEM que utilice, debería especificar algunas configuraciones adicionales del destinatario.

La figura siguiente muestra la pantalla de configuración del destinatario en ArcSight.




Configuración del destinatario en ArcSight

### Analizador sintáctico de mensajes

Los eventos exportados se transfieren al sistema SIEM en forma de mensajes. Estos mensajes deben analizarse; de lo contrario, el sistema SIEM no puede hacer uso de la información de los eventos. Los analizadores sintácticos de mensajes son parte del sistema SIEM; se usan para separar los contenidos del mensaje en los campos relevantes; por ejemplo, ID del evento, gravedad, descripción y parámetros. Esto permite al sistema SIEM procesar eventos recibidos de Kaspersky Security Center, de modo que se puedan almacenar en la base de datos del sistema SIEM.

## Marcar los eventos que se exportarán a un sistema SIEM en formato Syslog

Después de habilitar la exportación automática de eventos, debe seleccionar qué eventos se exportarán al sistema SIEM externo.

Para configurar la exportación de eventos en formato Syslog a un sistema externo, puede optar por una de estas vías:

- Marcar eventos generales. Si marca los eventos que desea exportar en la configuración de una directiva, en la configuración de los eventos o en la configuración del Servidor de administración, el sistema SIEM recibirá esos eventos cuando ocurran en cualquier aplicación sujeta a la directiva. Si los eventos exportados ya estaban seleccionados en la directiva, no podrá redefinirlos para una aplicación específica que esté administrada por esa directiva.

- Marcar eventos correspondientes a una aplicación administrada. Si marca eventos que correspondan a una aplicación administrada instalada en un dispositivo administrado, el sistema SIEM únicamente recibirá los eventos que ocurran en esa aplicación.

### Acerca del marcado de los eventos que se exportarán a un sistema SIEM en formato Syslog

Después de habilitar la exportación automática de eventos, debe seleccionar qué eventos se exportarán al sistema SIEM externo.

Para configurar la exportación de eventos en formato Syslog a un sistema externo, puede optar por una de estas vías:

- Marcar eventos generales. Si marca los eventos que desea exportar en la configuración de una directiva, en la configuración de los eventos o en la configuración del Servidor de administración, el sistema SIEM recibirá esos eventos cuando ocurran en cualquier aplicación sujeta a la directiva. Si los eventos exportados ya estaban seleccionados en la directiva, no podrá redefinirlos para una aplicación específica que esté administrada por esa directiva.

- Marcar eventos correspondientes a una aplicación administrada. Si marca eventos que correspondan a una aplicación administrada instalada en un dispositivo administrado, el sistema SIEM únicamente recibirá los eventos que ocurran en esa aplicación.

## Marcar eventos de una aplicación de Kaspersky para que se los exporte en formato Syslog

Si desea exportar los eventos ocurridos en una aplicación administrada específica instalada en los dispositivos administrados, marque los eventos para su exportación en la directiva de la aplicación. En este caso, los eventos marcados se exportan desde todos los dispositivos incluidos en el alcance de la directiva.

*Para marcar los eventos que desea exportar en una aplicación administrada específica, haga lo siguiente:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en la directiva de la aplicación para la que desea marcar los eventos.

   Se abre la ventana de configuración de la directiva.
3. Vaya a la sección **Configuración de eventos**.
4. marque las casillas ubicadas al lado de los eventos que quiera exportar a un sistema SIEM.
5. Haga clic en el botón **Marcar para exportar al sistema SIEM mediante Syslog**.

   > También puede marcar un evento para exportarlo a un sistema SIEM en la sección **Registro de los eventos**, que se abre al hacer clic en el vínculo del evento.

6. Aparecerá una marca de verificación (✓) en la columna **Syslog** del evento (o los eventos) que haya elegido exportar al sistema SIEM.
7. Haga clic en el botón **Guardar**.

Los eventos marcados desde la aplicación administrada están listos para ser exportados a un sistema SIEM.

Puede marcar los eventos que desea exportar a un sistema SIEM para un dispositivo administrado específico. Si se marcaron eventos previamente exportados en una directiva de aplicación, no podrá redefinir los eventos marcados para un dispositivo administrado.

*Para marcar los eventos que desea exportar a un dispositivo administrado, haga lo siguiente:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo pertinente.

   Se muestra la ventana de propiedades del dispositivo seleccionado.

3. Vaya a la sección **Aplicaciones**.

4. En la lista de aplicaciones, haga clic en el vínculo con el nombre de la aplicación en cuestión.

5. Vaya a la sección **Configuración de eventos**.

6. Active las casillas de verificación ubicadas junto a los eventos que deban exportarse al sistema SIEM.

7. Haga clic en el botón **Marcar para exportar al sistema SIEM mediante Syslog**.

   También puede marcar un evento para exportarlo a un sistema SIEM en la sección **Registro de los eventos**, que se abre al hacer clic en el vínculo del evento.

8. Aparecerá una marca de verificación (✓) en la columna **Syslog** del evento (o los eventos) que haya elegido exportar al sistema SIEM.

En lo sucesivo, si la exportación a un sistema SIEM está configurada, el Servidor de administración enviará los eventos marcados a ese sistema SIEM.

## Marcar eventos generales para que se los exporte en formato Syslog

Si lo desea, puede marcar eventos generales para que el Servidor de administración los exporte a sistemas SIEM en formato Syslog.

*Para marcar eventos generales y exportarlos a un sistema SIEM:*

1. Realice una de las siguientes acciones:

   - En el menú principal, haga clic en el icono de configuración (⚙) ubicado junto al nombre del Servidor de administración pertinente.
   - En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles** y haga clic en el vínculo de una directiva.

2. En la ventana que se abre, vaya a la pestaña **Configuración de eventos**.

3. Haga clic en **Marcar para exportar al sistema SIEM mediante Syslog**.

   Como alternativa, para marcar un evento que desee exportar al sistema SIEM, puede utilizar la sección **Registro de los eventos** que se abre al hacer clic en el vínculo del evento en cuestión.

4. Aparecerá una marca de verificación (✓) en la columna **Syslog** del evento (o los eventos) que haya elegido exportar al sistema SIEM.

En lo sucesivo, si la exportación a un sistema SIEM está configurada, el Servidor de administración enviará los eventos marcados a ese sistema SIEM.

## Acerca de la exportación de eventos en formato CEF o LEEF

Los eventos generales y los eventos que las aplicaciones de Kaspersky transfieren al Servidor de administración se pueden exportar al sistema SIEM en los formatos CEF y LEEF. El conjunto de eventos exportados se predefine, y no puede seleccionar los eventos que se exportarán. Antes de enviar eventos al sistema SIEM (QRadar, ArcSight o Splunk), es necesario interpretar los eventos de Kaspersky Security Center en eventos en formato CEF y LEEF mediante las reglas especificadas en el archivo siem_conversion_rules.xml.

Según el sistema SIEM que utilice, deberá elegir uno u otro formato de exportación. La siguiente tabla muestra los formatos correspondientes a algunos sistemas SIEM.

Formatos de exportación de eventos por sistema SIEM

| Sistema SIEM | Formato de exportación |
|---|---|
| QRadar | LEEF |
| ArcSight | CEF |
| Splunk | CEF |

- LEEF (Log Event Extended Format) es un formato de evento personalizado para IBM Security QRadar SIEM. QRadar puede integrar, identificar y procesar eventos LEEF. Los eventos LEEF deben usar la codificación de caracteres UTF-8. Puede encontrar la información detallada del protocolo LEEF en el Centro de conocimientos de IBM.

- CEF (Formato de eventos comunes) es un estándar abierto para la gestión de registros que mejora el interoperabilidad de la información relacionada con la seguridad desde diferentes dispositivos y aplicaciones de red y seguridad. CEF le permite usar un formato de registros de eventos común de modo que los datos se puedan integrar y agregarse fácilmente para el análisis por un sistema de gestión de la empresa. Los eventos CEF deben usar la codificación de caracteres UTF-8.

La exportación automática significa que Kaspersky Security Center envía eventos generales al sistema SIEM. La exportación automática de eventos se inicia inmediatamente después de que la habilita. Esta sección explica detalladamente cómo habilitar la exportación automática de eventos.

## Conversión de eventos al formato CEF o LEEF

Antes de enviar eventos al sistema SIEM (QRadar, ArcSight o Splunk), es necesario interpretar los eventos de Kaspersky Security Center en eventos en formato CEF y LEEF utilizando las reglas especificadas en el archivo siem_conversion_rules.xml. Este archivo está incluido en el kit de distribución de Kaspersky Security Center.

El archivo siem_conversion_rules.xml contiene las reglas de interpretación predefinidas para convertir eventos al formato CEF y LEEF. Si desea utilizar reglas de interpretación de eventos adicionales, puede agregarlas al archivo manualmente.

El archivo siem_conversion_rules.xml incluye las secciones `<product name="SP_QRADAR" vendor="IBM">` y `<product name="SP_QRADAR" vendor="IBM">`. La sección `<product name="SP_QRADAR" vendor="IBM">` contiene reglas para generar eventos en formato LEEF, que se pueden exportar al sistema SIEM de QRadar. La sección `<product name="SP_ARCSIGHT" vendor="HP">` contiene reglas para generar eventos en formato CEF, que se pueden exportar al sistema SIEM de QRadar.

Cada sección tiene la subsección <common> donde se encuentran los atributos de eventos de Kaspersky Security Center y los atributos correspondientes de los eventos en formato LEEF. Estos atributos comunes se utilizan para todos los tipos de eventos que se pueden exportar.

Además, cada sección tiene las subsecciones <event>. Cada subsección <event> contiene atributos adicionales que se agregan a los enumerados en la sección <common>.

Puede agregar una nueva regla de generación de eventos al archivo siem_conversion_rules.xml manualmente.

*Para agregar una nueva regla de generación de eventos:*

1. Agregar una nueva subsección <event> a la sección <product name="SP_QRADAR" vendor="IBM"> o <product name="SP_QRADAR" vendor="IBM">y, a continuación, especifique los atributos de evento adicionales, si es necesario.

2. Si un evento consta únicamente de atributos comunes, la subsección <event> estará vacía.

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Atributos de eventos comunes de Kaspersky Security Center y atributos de eventos LEEF
correspondientes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- Regla de generación para el evento GNRL_EV_VIRUS_FOUND con atributos
adicionales -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Atributos de eventos comunes de Kaspersky Security Center y atributos de eventos LEEF
correspondientes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

## Acerca de la exportación de eventos en formato Syslog

Los eventos del Servidor de administración y los eventos de las aplicaciones de Kaspersky que se encuentran instaladas en los dispositivos administrados se pueden exportar a un sistema SIEM en formato Syslog.

Syslog es un protocolo de registro de mensajes estándar. Permite que el software que genera los mensajes, el sistema que los almacena y el software que los reporta y analiza sean entidades separadas. Cada mensaje se etiqueta con un código numérico que indica el tipo de software que lo ha generado. A cada mensaje se le asigna, además, un nivel de gravedad.

La definición del formato Syslog se encuentra publicada en documentos RFC del Grupo de Trabajo de Ingeniería de Internet o IETF (estándares de Internet). El estándar RFC 5424 es usado para exportar los eventos desde Kaspersky Security Center a sistemas externos.

En Kaspersky Security Center, puede configurar la exportación de eventos a sistemas externos usando el formato Syslog.

El proceso de exportación consta de dos pasos:

1. Habilitar la exportación de eventos automática. En este paso, Kaspersky Security Center se configura de modo que envíe eventos al sistema SIEM. Kaspersky Security Center empieza a enviar eventos inmediatamente después de que habilita la exportación automática.

2. Seleccionar los eventos que se exportarán al sistema externo. Este paso consiste en indicar cuáles eventos deberán exportarse al sistema SIEM.

## Configurar Kaspersky Security Center para exportar eventos a un sistema SIEM

Si desea exportar eventos a un sistema SIEM, debe configurar el proceso de exportación en Kaspersky Security Center Web Console.

Antes de enviar eventos al sistema SIEM (QRadar, ArcSight o Splunk), es necesario interpretar los eventos de Kaspersky Security Center en eventos en formato CEF y LEEF utilizando las reglas especificadas en el archivo siem_conversion_rules.xml.

*Para configurar la exportación de eventos a un sistema SIEM en Kaspersky Security Center Web Console:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, seleccione la sección **Exportar a SIEM**.

3. Haga click en el enlace **Configuración**.

   Se abre la sección **Exportar configuración**.

4. En la sección **Exportar configuración**, configure los siguientes ajustes:

- **Dirección del servidor del sistema SIEM**

  La dirección IP del servidor en el que está instalado el sistema SIEM. Encontrará este valor en la configuración del sistema SIEM.

- **Puerto del sistema SIEM**

  El número de puerto usado para establecer una conexión entre Kaspersky Security Center y su servidor del sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center y en la configuración del destinatario de su sistema SIEM.

- **Protocolo**

Seleccione el protocolo que se utilizará para transferir mensajes al sistema SIEM. Puede seleccionar los protocolos TCP, UDP o TLS sobre TCP.

Si selecciona el protocolo TLS sobre TCP, configure los siguientes ajustes:

- **Autenticación del servidor**

  En el campo **Autenticación del servidor**, puede seleccionar los valores **Certificados de confianza** o **Huellas digitales SHA**:

  - **Certificados de confianza**. Puede obtener una cadena de certificados completa (incluido el certificado raíz) de una entidad de certificación (CA) de confianza y cargar ese archivo a Kaspersky Security Center. Kaspersky Security Center verifica si la cadena de certificados del servidor del sistema SIEM también está firmado por una CA de confianza o no.

    Para agregar un certificado de confianza, haga clic en el botón **Buscar archivo de certificados de CA** y, a continuación, cargue el certificado en cuestión.

  - **Huellas digitales SHA**. Puede especificar las huellas digitales SHA1 de la cadena de certificados completa del sistema SIEM (incluido el certificado raíz) en Kaspersky Security Center. Para agregar una huella digital SHA1, cópiela en el campo **Huellas digitales** y haga clic en el botón **Agregar**.

  La opción **Agregar autenticación del cliente** permite generar un certificado para autenticar a Kaspersky Security Center. Si utiliza esta opción, utilizará un certificado autofirmado emitido por Kaspersky Security Center. En ese caso, podrá usar tanto un certificado de confianza como una huella digital SHA para autenticar al servidor del sistema SIEM.

- **Agregar nombre del sujeto / nombre alternativo del sujeto**

  Se denomina "nombre del sujeto" al nombre de dominio para el que se ha obtenido un certificado. Para que Kaspersky Security Center pueda conectarse al servidor del sistema SIEM, el nombre de dominio del servidor del sistema SIEM debe aparecer como nombre del sujeto en el certificado del servidor del sistema SIEM. El servidor del sistema SIEM puede cambiar de nombre de dominio si se modifica también el nombre del sujeto en el certificado. Si se presenta esta situación, utilice el campo **Agregar nombre del sujeto / nombre alternativo del sujeto** para especificar los nombres de sujeto pertinentes. Si alguno de los nombres de sujeto indicados en el campo coincide con el nombre de sujeto especificado en el certificado del sistema SIEM, Kaspersky Security Center considerará que el certificado es válido.

- **Agregar autenticación del cliente**

  Para la autenticación del cliente, puede utilizar su propio certificado o generar uno en Kaspersky Security Center.

  - **Ingresar certificado**. Puede utilizar un certificado obtenido de cualquier fuente (por ejemplo, de una entidad de certificación de confianza). Deberá especificar el certificado y su clave privada. Puede usar, para ello, alguno de los siguientes tipos de certificado:

    - **PEM certificado X.509**. Use el campo **Archivo con certificado** para cargar el archivo que contenga el certificado y el campo **Archivo con clave** para cargar un archivo que contenga la clave privada. Los archivos no dependen el uno del otro y no importa el orden en que se los carga. Tras cargar los archivos, ingrese la contraseña para decodificar la clave privada en el campo **Verificación de certificado o contraseña**. Si la clave privada no está codificada, puede dejar la contraseña en blanco.

    - **PKCS12 certificado X.509**. Use el campo **Archivo con certificado** para cargar un único archivo que contenga tanto el certificado como su clave privada. Tras cargar el archivo, ingrese la contraseña para decodificar la clave privada en el campo **Verificación de certificado o contraseña**. Si la clave privada no está codificada, puede dejar la contraseña en blanco.

- **Generar clave**. Puede generar un certificado autofirmado dentro de Kaspersky Security Center. El certificado autofirmado que se genere quedará almacenado en Kaspersky Security Center, y usted podrá transferir la parte pública del certificado o su huella digital SHA-1 al sistema SIEM.

- Formato de los datos

  Dependiendo de los requisitos del sistema SIEM, puede usar los formatos de System log, CEF o LEEF.

Si selecciona el formato de datos System log, debe especificar lo siguiente:

- Tamaño máximo de mensaje, bytes

  Especifique el tamaño máximo (en bytes) de un mensaje transmitido al sistema SIEM. Cada evento se transmite en un mensaje. Si la duración real de un mensaje supera el valor especificado, el mensaje es truncado y los datos se pueden perder. El tamaño predeterminado es de 2048 bytes. Este campo solo está disponible si seleccionó el formato de System log en el campo **Protocolo**.

5. Si lo desea, puede exportar eventos que se encuentren archivados en la base de datos del Servidor de administración y definir la fecha a partir de la cual se iniciará la exportación de los eventos archivados:

   a. Haga clic en el vínculo **Establezca la fecha de inicio de la exportación**.

   b. En la sección que se abre, especifique la fecha de inicio en el campo **Fecha de inicio de la exportación de eventos del sistema**.

   c. Haga clic en el botón **Aceptar**.

6. Cambie la opción a la posición **Exportar eventos a la base de datos del sistema SIEM automáticamente Habilitado**.

7. Para comprobar que la conexión del sistema SIEM se haya configurado correctamente, haga clic en el botón **Comprobar conexión**.

   Se establece la conexión con el servidor del sistema SIEM y se envía un evento de prueba. Se mostrará el estado de la conexión.

   La verificación se realiza solo para TCP/IP y TLS a través de protocolos TCP.

8. Haga clic en el botón **Guardar**.

La exportación de eventos al sistema SIEM queda configurada.

## Exportación de eventos directamente desde la base de datos

Puede recuperar eventos directamente desde la base de datos de Kaspersky Security Center sin necesidad de usan la interfaz de Kaspersky Security Center. Puede consultar directamente las vistas públicas y recuperar los datos del evento o crear su propia vista a partir de vistas públicas existentes y dirigirse a ellas para obtener los datos que necesita.

## Vistas públicas

Para su conveniencia, un conjunto de vistas públicas se proporciona en la base de datos de Kaspersky Security Center. Puede encontrar la descripción de estas vistas públicas en el documento klakdb.chm.

La vista pública v_akpub_ev_event contiene un conjunto de campos que representan los parámetros del evento en la base de datos. En el documento klakdb.chm, también puede encontrar información sobre las vistas públicas correspondiente a otras entidades de Kaspersky Security Center; por ejemplo, dispositivos, aplicaciones o usuarios. Puede usar esta información en sus consultas.

Esta sección contiene instrucciones para ejecutar una consulta SQL mediante la utilidad klsql2 y un ejemplo de consulta.

Para crear consultas SQL o vistas de bases de datos, también puede utilizar cualquier otro programa para trabajar con bases de datos. En la sección correspondiente, se proporciona información sobre cómo ver los parámetros para conectar a la base de datos de Kaspersky Security Center, como el nombre de la instancia y nombre de la base de datos.

## Ejecución de una consulta SQL mediante la utilidad klsql2

En este artículo se describe cómo descargar y usar la utilidad klsql2, y cómo ejecutar una consulta SQL mediante esta utilidad.

*Para usar la utilidad klsql2:*

1. Inicie la utilidad klsrvswch desde la carpeta de instalación de Kaspersky Security Center. La ruta de instalación predeterminada es <Disk>:\Archivos de programa(x86)\Kaspersky Lab\Kaspersky Security Center. No utilice versiones de la utilidad klsql2 diseñadas para versiones anteriores de Kaspersky Security Center.

2. Cree un archivo con la extensión src.sql en cualquier editor de texto y póngalo en la misma carpeta que la utilidad.

3. En el archivo .sql creado, escriba la consulta SQL que desea, y luego, guarde el archivo.

4. En el dispositivo que tiene instalado el Servidor de administración de Kaspersky Security Center, en la línea de comandos, escriba el siguiente comando para ejecutar la consulta SQL desde el archivo .sql y guardar los resultados en el archivo result.xml:
   ```
   [[klsql2 -i src.sql -u <]] nombre de usuario[[> -p <]] contraseña[[> -o result.xml]]
   ```
   dónde < `nombre de usuario` > y < `contraseña` > son credenciales de la cuenta de usuario que tiene acceso a la base de datos.

5. Si es necesario, ingrese el nombre de usuario y la contraseña de la cuenta de usuario que tiene acceso a la base de datos.

6. Abra los archivos result.xml creados recientemente para ver los resultados de la consulta SQL.

Puede modificar el archivo .sql y crear cualquier consulta SQL para las vistas públicas. A continuación, desde la línea de comandos, ejecute su consulta SQL y guarde los resultados en un archivo.

## Ejemplo de una consulta de SQL usando la utilidad klsql2

Esta sección muestra un ejemplo de una consulta SQL, ejecutada por medio de la utilidad klsql2.

Los ejemplos siguientes ilustran la recuperación de eventos que ocurrieron en dispositivos durante los siete días anteriores, y muestran los eventos según la hora en la que se producen. Los eventos más recientes se muestran primero.

Ejemplo para Microsoft SQL Server:

```
SELECT
  /* identificador del evento */
  e.nId,

  /* hora en la que ocurrió el evento */
  e.tmRiseTime,

  /* nombre interno del tipo de evento */
  e.strEventType,

  /* nombre mostrado del evento */
  e.wstrEventTypeDisplayName,

  /* descripción mostrada del evento */
  e.wstrDescription,

  /* nombre del grupo donde se encuentra el dispositivo */
  e.wstrGroupName,

  /* nombre mostrado del dispositivo en el que ocurrió el evento */
  h.wstrDisplayName,
  CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

  /* Dirección IP del dispositivo en el que ocurrió el evento */
  CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
  INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Ejemplo para PostgreSQL:

```
SELECT
  /* identificador del evento */
  "e"."nId",

  /* hora en que ocurrió el evento */
  "e"."tmRiseTime",

  /* nombre interno del tipo de evento */
  "e"."strEventType",

  /* nombre mostrado del evento */
  "e"."wstrEventTypeDisplayName",

  /* descripción mostrada del evento */
  "e"."wstrDescription",

  /* descripción mostrada del evento */
  "e"."wstrGroupName",

  /* nombre mostrado del dispositivo en el que ocurrió el evento */
  "h"."wstrDisplayName",
  (
    CAST(("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST(("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST(("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* Dirección IP del dispositivo en el que ocurrió el evento */
    CAST(("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

Ejemplo para MySQL o MariaDB

```
SELECT

  /* identificador del evento */
  `e`.`nId`,

  /* hora en que ocurrió el evento */
  `e`.`tmRiseTime`,

  /* nombre interno del tipo de evento */
  `e`.`strEventType`,

  /* nombre mostrado del evento */
  `e`.`wstrEventTypeDisplayName`,

  /* descripción mostrada del evento */
  `e`.`wstrDescription`,

  /* nombre del grupo del dispositivo */
  `e`.`wstrGroupName`,

  /* nombre mostrado del dispositivo en el que ocurrió el evento */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* Dirección IP del dispositivo en el que ocurrió el evento */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

### Visualización del nombre de la base de datos de Kaspersky Security Center

Si desea acceder a la base de datos de Kaspersky Security Center por medio de las herramientas de administración de bases de datos de SQL Server, MySQL o MariaDB, debe conocer el nombre de la base de datos a fin de conectarse desde su editor de scripts SQL.

*Para ver el nombre de la base de datos de Kaspersky Security Center:*

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, seleccione la sección **Detalles de la base de datos actual**.

El nombre de la base de datos se especifica en el campo **Nombre de la base de datos**. Use el nombre de la base de datos para dirigirse a la base de datos en sus consultas de SQL.

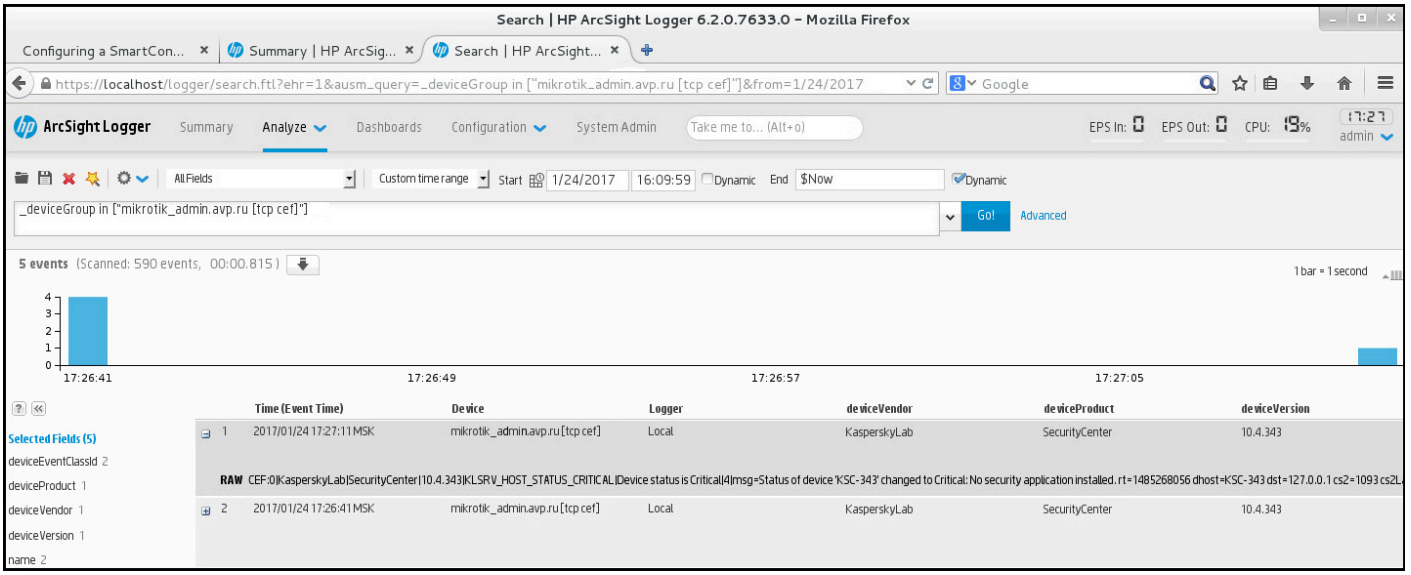
## Ver los resultados de la exportación

Puede controlar si el procedimiento de exportación de eventos se ha completado debidamente. Para ello, verifique si el sistema SIEM recibe mensajes con los eventos exportados.

Si los eventos enviados desde Kaspersky Security Center se reciben y analizan correctamente en su sistema SIEM, la configuración a ambos lados se realizó correctamente. De lo contrario, verifique la configuración que especificó en Kaspersky Security Center en comparación con la configuración en su sistema SIEM.

La imagen de más abajo muestra los eventos exportados a ArcSight. El primero de ellos, *Device status is Critical*, es un evento crítico del Servidor de administración que se refiere al estado de un dispositivo.

La representación de los eventos exportados a un sistema SIEM varía según el sistema SIEM utilizado.




Ejemplo de eventos

# Cómo trabajar con Kaspersky Security Center Web Console en un entorno de nube

Esta sección proporciona información sobre las funciones de Kaspersky Security Center Web Console relacionadas con el despliegue y el mantenimiento de Kaspersky Security Center en un entorno de nube, como Amazon Web Services, Microsoft Azure o Google Cloud.

Para operar en un entorno de nube, se necesita una licencia especial. Si no cuenta con esta licencia, no verá los elementos de la interfaz vinculados a los dispositivos de nube.

# Configuración del entorno de nube en Kaspersky Security Center Web Console

Para configurar Kaspersky Security Center mediante el Asistente de configuración del entorno de nube, debe tener lo siguiente:

- Las credenciales específicas de un entorno de nube:
  - Una función de IAM a la que se le haya otorgado el derecho de sondear el segmento de la nube o una cuenta de usuario de IAM a la que se le haya otorgado el derecho de sondear el segmento de la nube (para trabajar con Amazon Web Services)
  - Id. de aplicación, contraseña y suscripción de Azure (para operar con Microsoft Azure)
  - Correo electrónico del cliente, id. de proyecto y clave privada de Google (para operar con Google Cloud)
- Paquetes de instalación:
  - Agente de red para Windows
  - Agente de red para Linux
  - Kaspersky Endpoint Security for Linux
- Complemento web para Kaspersky Endpoint Security for Linux
- Al menos uno de los siguientes:
  - Paquete de instalación y complemento web para Kaspersky Endpoint Security para Windows (recomendado)
  - Paquete de instalación y complemento de administración de Kaspersky Security for Windows Server

Si realiza el despliegue de Kaspersky Security Center con una imagen lista para usar, la configuración del entorno de nube se abrirá automáticamente cuando se conecte al Servidor de administración por primera vez a través de la Consola de administración. También puede iniciar el asistente manualmente en cualquier momento.

*Para iniciar manualmente el Asistente del configuración del entorno de nube:*

En el menú principal, vaya a **Descubrimiento y despliegue** → **Despliegue y asignación** → **Configurar entorno de nube**.

Se inicia el asistente.

Una sesión de trabajo promedio para la configuración de un entorno en la nube dura unos 15 minutos.

## Paso 1. Comprobar los complementos y paquetes de instalación necesarios

Este paso no se muestra si tiene todos los complementos web y paquetes de instalación necesarios que se enumeran a continuación.

Para configurar un entorno de nube, debe tener los siguientes componentes:

- Paquetes de instalación:
  - Agente de red para Windows
  - Agente de red para Linux
  - Kaspersky Endpoint Security for Linux
- Complemento web para Kaspersky Endpoint Security for Linux
- Al menos uno de los siguientes:
  - Paquete de instalación y complemento web para Kaspersky Endpoint Security para Windows (recomendado)
  - Paquete de instalación y complemento de administración de Kaspersky Security for Windows Server

    Le recomendamos que utilice Kaspersky Endpoint Security para Windows en lugar de Kaspersky Security for Windows Server.

Kaspersky Security Center Cloud Console detecta automáticamente los componentes que ya tiene y enumera solo los que faltan. Para descargar los componentes enumerados, haga clic en el botón **Seleccionar aplicaciones para descargar** y luego seleccione los complementos y paquetes de instalación requeridos. Después de descargar un componente, puede utilizar el botón **Actualizar** para actualizar la lista de componentes que faltan.

## Paso 2. Obtención de licencias de la aplicación

Verá este paso únicamente si está utilizando una AMI pensada para la modalidad BYOL ("traiga su propia licencia") y si no ha activado la aplicación con una licencia de Kaspersky Security for Virtualization o una licencia de Kaspersky Hybrid Cloud Security.

Especifique la clave de licencia y haga clic en **Siguiente** para procesar.

La clave de licencia se agrega al repositorio del Servidor de administración.

Si vuelve a ejecutar el asistente, este paso no se muestra.

# Paso 3. Selección del entorno de nube y autorización

Esta sección describe las funciones correspondientes solo a Kaspersky Security Center 12.1 o una versión posterior.

Configure los siguientes ajustes:

- **Entorno de nube**

  Seleccione el entorno de nube en el que va a realizar el despliegue de Kaspersky Security Center: AWS, Azure o Google Cloud.

  Si planea trabajar con más de un entorno de nube, seleccione uno en este momento y vuelva a ejecutar el asistente más tarde.

- **Nombre de conexión**

  Escriba un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres Unicode.

  El nombre que escriba aquí será también el nombre del grupo de administración para los dispositivos de nube.

  Si planea trabajar con más de un entorno de nube, sugerimos que incluya el nombre del entorno en el nombre de la conexión (por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google").

Introduzca las credenciales para autorizarse en el entorno de nube seleccionado.

## AWS

Si selecciona AWS como tipo de segmento de la nube, necesitará una función de IAM o una clave de acceso de AWS IAM para permitir el sondeo del segmento.

- **Función de AWS IAM asignada a una instancia de EC2**

  Seleccione esta opción si ha creado una función de IAM con los derechos necesarios para el Servidor de administración.

- **Usuario de AWS IAM**

  Seleccione esta opción si cuenta con una clave de acceso de AWS IAM. Escriba los datos de la clave:

  - **Id. de clave de acceso**

    El id. de la clave de acceso de IAM es una secuencia de caracteres alfanuméricos. Obtuvo este id. al crear la cuenta de usuario de IAM.

    El campo está disponible si seleccionó una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

  - **Clave secreta**

    La clave secreta que recibió con el id. de la clave de acceso al crear la cuenta de usuario de IAM.

    Los caracteres de la clave secreta se muestran como asteriscos. Cuando comience a escribir la clave secreta, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado el tiempo que necesite para ver los caracteres introducidos.

    El campo está disponible si seleccionó una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

    Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

## Azure

Si ha seleccionado Azure como tipo de segmento de nube, debe introducir los siguientes datos para permitir el sondeo del segmento:

- **Id. de la aplicación en Azure**

  Usted creó el id. de la aplicación en el portal de Azure.

  No puede especificar más de un id. de aplicación de Azure para realizar sondeos u otros fines. Si desea sondear otro segmento de Azure, elimine primero la conexión de Azure existente.

- **Id. de suscripción de Azure**

  Creó esta suscripción en el portal de Azure.

- **Contraseña de la aplicación en Azure**

  Recibió la contraseña correspondiente al id. de aplicación cuando creó dicho id.

  Los caracteres de la contraseña se muestran como asteriscos. Cuando empiece a introducir la contraseña, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado para ver los caracteres introducidos.

  Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

- **Nombre de la cuenta de almacenamiento de Azure**

  Usted creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

- **Clave de acceso al almacenamiento de Azure**

  Recibió una contraseña (clave) cuando creó la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

  La clave está disponible en la sección "Overview of the Azure storage account" ("Descripción general de la cuenta de almacenamiento de Azure"), subsección "Keys" ("Claves").

  Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

### Google Cloud

Si ha seleccionado Google Cloud como tipo de segmento de nube, debe introducir los siguientes datos para permitir el sondeo del segmento:

- **Correo electrónico del cliente**

  La dirección de correo electrónico que utilizó para registrar su proyecto en Google Cloud.

- **Id. de proyecto**

  El id. que le enviaron cuando registró su proyecto en Google Cloud.

- **Clave privada**

  La secuencia de caracteres que le enviaron como clave privada cuando registró su proyecto en Google Cloud. Recomendamos que copie y pegue esta secuencia para evitar errores.

  Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

La aplicación guarda la conexión configurada.

El Asistente de configuración del entorno de nube solo permite especificar un segmento. Si necesita administrar otros segmentos de nube, podrá agregar las conexiones necesarias en otro momento.

Haga clic en **Siguiente** para continuar.

## Paso 4. Sondeo del segmento, opciones de sincronización con la nube y otras acciones

En este paso, la aplicación comienza a sondear el segmento de la nube y crea automáticamente un grupo de administración especial para los dispositivos de nube. Los dispositivos que se detecten durante el sondeo se agregarán a este nuevo grupo. De manera predeterminada, el proceso de sondeo se repetirá cada 5 minutos; si desea cambiar este valor, podrá hacerlo más adelante.

La aplicación también creará una regla de movimiento automático llamada **Sincronizar con la nube**. Para cada análisis posterior de la red en la nube, los dispositivos virtuales detectados se moverán al subgrupo correspondiente dentro del grupo **Dispositivos administrados\Nube**.

Defina los siguientes parámetros de configuración:

- **Sincronizar los grupos de administración con la estructura de nube**

  Si habilita está opción, se creará el grupo **Cloud** automáticamente dentro el grupo **Dispositivos administrados** y se iniciará un proceso para descubrir dispositivos en la nube. Las instancias y las máquinas virtuales que se detecten cada vez que se sondee la red de la nube se agregarán al grupo "Cloud". La estructura de subgrupos de administración dentro de este grupo se hará coincidir con la estructura del segmento de la nube (en AWS, las zonas de disponibilidad y los grupos de ubicación no estarán representados en la estructura; en Azure, no estarán representadas las subredes). Los dispositivos que no se hayan identificado como instancias en el entorno de nube estarán en el grupo **Dispositivos no asignados**. Esta estructura de grupo le permite usar tareas de instalación en grupo para instalar aplicaciones antivirus en instancias, así como configurar diferentes directivas para diferentes grupos.

  Si no habilita esta opción, también se creará el grupo **Cloud** y también se iniciará el descubrimiento de dispositivos de la nube, pero no se crearán subgrupos que coincidan con la estructura del segmento de la nube dentro del grupo. Todas las instancias detectadas se agregarán al grupo de administración **Cloud** y aparecerán en una misma lista. Si su trabajo con Kaspersky Security Center requiere sincronización, puede modificar las propiedades de la regla **Sincronizar con Cloud** y aplicarla. Al aplicar la regla, la estructura de subgrupos del grupo "Cloud" se hará coincidir con la estructura del segmento de la nube.

  Esta opción está deshabilitada de forma predeterminada.

- **Desplegar protección**

  Si se selecciona esta opción, el asistente crea una tarea para instalar aplicaciones de seguridad en instancias. Una vez que finalice el asistente, el Asistente de despliegue de la protección se inicia automáticamente en los dispositivos de sus segmentos de nube, y usted podrá instalar el Agente de red y las aplicaciones de seguridad en esos dispositivos.

  Kaspersky Security Center puede realizar el despliegue con sus herramientas nativas. Si no tiene permisos para instalar las aplicaciones en instancias EC2 o máquinas virtuales de Azure, puede configurar la tarea **Instalación remota** manualmente y especificar una cuenta con los permisos requeridos. En este caso, la tarea de instalación remota no funcionará para los dispositivos detectados utilizando la API de AWS o Azure. Esta tarea solo funciona para los dispositivos descubiertos mediante el sondeo de Active Directory, el sondeo de dominios de Windows o el sondeo de rango de IP.

  Si esta opción no está seleccionada, el Asistente de despliegue de la protección no se inicia y no se crean tareas para instalar las aplicaciones de seguridad en las instancias. Puede realizar manualmente ambas acciones más adelante.

Si selecciona la opción Desplegar protección, se habilitará una sección llamada **Reinicio de dispositivos**. Indique allí qué hacer cuando se necesite reiniciar el sistema operativo de un dispositivo de destino. Seleccione si reiniciar instancias si el sistema operativo de su dispositivo debe reiniciarse durante la instalación de aplicaciones:

- **No reiniciar**

  Si se selecciona esta opción, el dispositivo no se reiniciará después de instalar la aplicación de seguridad.

- **Reiniciar**

  Si se selecciona esta opción, el dispositivo se reiniciará después de instalar la aplicación de seguridad.

Haga clic en **Siguiente** para continuar.

Para Google Cloud, solo puede realizar el despliegue con herramientas propias de Kaspersky Security Center. Si seleccionó Google Cloud, la opción **Desplegar protección** no estará disponible.

## Paso 5. Seleccionar una aplicación para crear una directiva y tareas

Este paso solo se muestra si tiene paquetes de instalación y complementos para Kaspersky Endpoint Security para Windows y Kaspersky Security for Windows Server. Si tiene un complemento y un paquete de instalación solo para una de esas aplicaciones, este paso se omite y Kaspersky Security Center Cloud Console crea una directiva y tareas para la aplicación existente.

Seleccione una aplicación para la que desea crear una directiva.

- Kaspersky Endpoint Security para Windows
- Kaspersky Security for Windows Server

## Paso 6. Configuración de Kaspersky Security Network para Kaspersky Security Center

Especifique la configuración para transmitir la información sobre operaciones Kaspersky Security Center a la base de conocimientos de Kaspersky Security Network (KSN). Seleccione una de las siguientes opciones:

- **Acepto utilizar Kaspersky Security Network**

  Kaspersky Security Center y las aplicaciones administradas instaladas en dispositivos cliente transferirán automáticamente su información de operación a Kaspersky Security Network. Participar en Kaspersky Security Network permite que las bases de datos con información sobre virus y otros riesgos se actualicen más rápidamente, lo cual se traduce en una mayor velocidad de respuesta ante amenazas a la seguridad emergentes.

- **No acepto utilizar Kaspersky Security Network**

  Kaspersky Security Center y las aplicaciones administradas no proporcionarán información a Kaspersky Security Network.

  Si selecciona esta opción, se deshabilitará el uso de Kaspersky Security Network.

Kaspersky recomienda participar en Kaspersky Security Network.

Es posible que se le muestren los acuerdos de KSN correspondientes a las aplicaciones administradas. Si acepta usar Kaspersky Security Network, las aplicaciones administradas remitirán información a Kaspersky. Si opta por no participar en Kaspersky Security Network, estas aplicaciones no enviarán información a Kaspersky. Si cambia de opinión en algún momento, podrá indicarlo a través de la directiva de la aplicación.

Haga clic en **Siguiente** para continuar.

## Paso 7. Creación de una configuración de protección inicial

Puede ver la lista de directivas y tareas creadas.

Espere a que finalice la creación de las tareas y directivas. A continuación, haga clic en **Siguiente**. En la última página del asistente, haga clic en el botón **Finalizar** para salir.

# Sondeo de segmentos de red con Kaspersky Security Center Web Console

El Servidor de administración recaba información sobre la estructura de la red, y sobre los dispositivos que la componen, realizando sondeos periódicos de los segmentos de nube. Estos sondeos se llevan a cabo a través de las herramientas que brindan las API de AWS, Azure y Google. Kaspersky Security Center usa esta información para actualizar los contenido de las carpetas Dispositivos no asignados y Dispositivos administrados. Si se han configurado reglas de movimiento automático, los dispositivos detectados se agregan a los grupos de administración que les corresponden automáticamente.

Para que el Servidor de administración pueda sondear segmentos de nube, necesitará contar con ciertos derechos, que pueden otorgarse a través de una función de IAM o una cuenta de usuario de IAM (en el caso de AWS), un id. de la aplicación y la contraseña de esa aplicación (en el caso de Azure) o un id. de proyecto, una clave privada y el correo electrónico del cliente (en el caso de Google Cloud).

Puede agregar y eliminar conexiones para cada segmento de nube y definir una programación de sondeo para cada segmento.

## Adición de conexiones para el sondeo de segmento de la nube

*Para agregar una conexión para sondear un segmento de nube a la lista de conexiones disponibles:*

1. En el menú principal, vaya a **Descubrimiento y despliegue** → **Descubrimiento** → **Cloud**.
2. En la ventana que se abre, haga clic en **Propiedades**.
3. En la ventana **Configuración** que se abre, haga clic en **Agregar**.

   Se abre la ventana **Configuración del segmento de la nube**.
4. Escriba el nombre del entorno de nube correspondiente a la conexión que se usará para sondear el segmento de nube:

   - **Entorno de nube**

     Seleccione el entorno de nube en el que va a realizar el despliegue de Kaspersky Security Center: AWS, Azure o Google Cloud.

     Si planea trabajar con más de un entorno de nube, seleccione uno en este momento y vuelva a ejecutar el asistente más tarde.

   - **Nombre de conexión**

     Escriba un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres Unicode.

     El nombre que escriba aquí será también el nombre del grupo de administración para los dispositivos de nube.

     Si planea trabajar con más de un entorno de nube, sugerimos que incluya el nombre del entorno en el nombre de la conexión (por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google").

5. Introduzca las credenciales para autorizarse en el entorno de nube seleccionado.

- Si seleccionó AWS, configure los siguientes parámetros:
  - **Usar función de AWS IAM**

    Elija esta opción si ha creado ya una función de IAM para que el Servidor de administración use servicios AWS.

  - **Credenciales de la cuenta de usuario de AWS IAM**

    Seleccione esta opción si tiene una cuenta de usuario de IAM con los permisos necesarios y puede ingresar un id. de clave y una clave secreta.

    Si elige la opción Credenciales de la cuenta de usuario de AWS IAM, introduzca los siguientes datos:

    - **Id. de clave de acceso**

      El id. de la clave de acceso de IAM es una secuencia de caracteres alfanuméricos. Obtuvo este id. al crear la cuenta de usuario de IAM.

      El campo está disponible si seleccionó una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

    - **Clave secreta**

      La clave secreta que recibió con el id. de la clave de acceso al crear la cuenta de usuario de IAM.

      Los caracteres de la clave secreta se muestran como asteriscos. Cuando comience a escribir la clave secreta, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado el tiempo que necesite para ver los caracteres introducidos.

      El campo está disponible si seleccionó una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

    Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

- Si seleccionó Azure, configure los siguientes parámetros:
  - **Id. de la aplicación en Azure**

    Usted creó el id. de la aplicación en el portal de Azure.

    No puede especificar más de un id. de aplicación de Azure para realizar sondeos u otros fines. Si desea sondear otro segmento de Azure, elimine primero la conexión de Azure existente.

  - **Id. de suscripción de Azure**

    Creó esta suscripción en el portal de Azure.

  - **Contraseña de la aplicación en Azure**

Recibió la contraseña correspondiente al id. de aplicación cuando creó dicho id.

Los caracteres de la contraseña se muestran como asteriscos. Cuando empiece a introducir la contraseña, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado para ver los caracteres introducidos.

Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

- **Nombre de la cuenta de almacenamiento de Azure**

  Usted creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

- **Clave de acceso de la cuenta de almacenamiento de Azure**

  Recibió una contraseña (clave) cuando creó la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

  La clave está disponible en la sección "Overview of the Azure storage account" ("Descripción general de la cuenta de almacenamiento de Azure"), subsección "Keys" ("Claves").

  Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

Si seleccionó Google Cloud, configure los siguientes ajustes:

- **Correo electrónico del cliente**

  La dirección de correo electrónico que utilizó para registrar su proyecto en Google Cloud.

- **Id. de proyecto**

  El id. que le enviaron cuando registró su proyecto en Google Cloud.

- **Clave privada**

  La secuencia de caracteres que le enviaron como clave privada cuando registró su proyecto en Google Cloud. Recomendamos que copie y pegue esta secuencia para evitar errores.

  Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

6. Si lo desea, haga clic en **Establecer programación de sondeo** y cambie la configuración predeterminada.

La conexión se guarda en la configuración de la aplicación.

Una vez que el nuevo segmento de la nube se haya sondeado por primera vez, el subgrupo correspondiente a ese segmento aparecerá en el grupo de administración **Dispositivos administrados\Nube**.

Si las credenciales que introdujo no son correctas, no se encontrará ninguna instancia durante el sondeo del segmento y, en consecuencia, no aparecerá ningún subgrupo nuevo en el grupo de administración **Dispositivos administrados\Cloud**.

## Eliminar conexiones para el sondeo de segmentos de nube

Si ya no necesita que la aplicación sondee un segmento de nube en particular, puede eliminar la conexión correspondiente a ese segmento de la lista de conexiones disponibles. Lo mismo puede hacer si, por ejemplo, los permisos para sondear el segmento se han transferido a un usuario que utiliza otras credenciales.

*Para eliminar una conexión:*

1. En el menú principal, vaya a **Descubrimiento y despliegue → Descubrimiento → Cloud**.
2. En la ventana que se abre, haga clic en **Propiedades**.
3. En la ventana **Configuración** que se abre, haga clic en el nombre del segmento que desee eliminar.
4. Haga clic en **Eliminar**.
5. En la ventana que se abre, haga clic en el botón **Aceptar** para confirmar su elección.

   La conexión se eliminará. Los dispositivos del segmento de nube asociado a la conexión se eliminarán automáticamente de los grupos de administración.

## Programación de sondeos a través de Kaspersky Security Center Web Console

El sondeo de segmentos de nube se realiza siguiendo una programación. Si lo desea, puede configurar la frecuencia con la que se llevan a cabo los sondeos.

La frecuencia de sondeo se establece automáticamente en 5 minutos en la configuración del entorno de nube. Puede cambiar este valor en cualquier momento y definir una programación diferente. Sin embargo, no se recomienda configurar el sondeo para que se ejecute con más frecuencia que cada 5 minutos, porque esto podría llevar a errores en la operación API.

*Para configurar la programación de sondeo para un segmento de nube:*

1. En el menú principal, vaya a **Descubrimiento y despliegue → Descubrimiento → Cloud**.
2. En la ventana que se abre, haga clic en **Propiedades**.
3. En la ventana **Configuración** que se abre, haga clic en el nombre del segmento para el que quiera configurar la programación de sondeo.

   Se abre la ventana **Configuración del segmento de la nube**.

4. En la ventana **Configuración del segmento de la nube**, haga clic en **Establecer programación de sondeo**.
   Se abre la ventana **Programación**.

5. En la ventana **Programación**, configure los siguientes ajustes:

- **Inicio programado**

  Opciones de programación para el sondeo:

  - **Cada N días**

    Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la fecha y hora indicadas. Cada sondeo estará separado del anterior por el número de días que indique.

    De forma predeterminada, se realizará un sondeo todos los días, a partir de la fecha y hora actuales del sistema.

  - Cada N minutos

    Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la hora indicada. Cada sondeo estará separado del anterior por el número de minutos que indique.

    De forma predeterminada, se realizará un sondeo cada cinco minutos, a partir de la hora actual del sistema.

  - Por días de la semana

    Se realizará un sondeo en forma periódica, a intervalos regulares, en el día de la semana y a la hora que indique.

    De manera predeterminada, el sondeo se ejecutará todos los viernes a las 18:00:00.

  - Cada mes en los días especificados de semanas seleccionadas

    Se realizará un sondeo en forma periódica, a intervalos regulares, en los días del mes y a la hora que indique.

    Por defecto, no hay ningún día seleccionado; la hora de inicio predeterminada es las 18:00:00.

- Intervalo de inicio

  Indique a cuántos días o minutos, según el caso, equivale N.

- Primera ejecución

  Indique cuándo se realizará el primer sondeo.

- Ejecutar tareas no realizadas

Si el Servidor de administración está apagado o no está disponible durante la hora programada para el sondeo, el Servidor de administración puede iniciar el sondeo inmediatamente después de encenderlo o esperar la próxima vez que se programe el sondeo.

Si esta opción está habilitada, el Servidor de administración inicia el sondeo inmediatamente después de que se enciende.

Si esta opción está desactivada, el Servidor de administración espera la próxima vez que se programe el sondeo.

Esta opción está activada de forma predeterminada.

6. Guarde los cambios.

La aplicación guarda la programación de sondeo para el segmento.

## Ver los resultados del sondeo de segmentos de nube en Kaspersky Security Center Web Console

Puede consultar los resultados del sondeo de sus segmentos de nube. Dicho de otro modo, puede ver la lista de dispositivos de nube administrados por el Servidor de administración.

*Para ver los resultados del sondeo de segmentos de nube:*

En el menú principal, vaya a **Descubrimiento y despliegue** → **Descubrimiento** → **Cloud**.

Verá los distintos segmentos de nube que la aplicación puede sondear.

## Visualización de las propiedades de dispositivos de nube en Kaspersky Security Center Web Console

Puede ver las propiedades de cada dispositivo de nube.

*Para ver las propiedades de un dispositivo de nube:*

1. En el menú principal, vaya a **Activos (dispositivos)**→ **Dispositivos administrados**.
2. Haga clic en el nombre del dispositivo en cuyas propiedades esté interesado.

   Se abrirá una ventana de propiedades con la sección **General** seleccionada.
3. Si desea ver las propiedades específicas de los dispositivos en la nube, seleccione la sección **Sistema** en la ventana de propiedades.

   Las propiedades que se muestran dependen de la plataforma de nube del dispositivo.

   Para los dispositivos en AWS, se muestran las siguientes propiedades:

   - **Dispositivo encontrado mediante API** (valor: **AWS**)
   - **Región de la nube**
   - **Cloud VPC**
   - **Zona de disponibilidad en la nube**
   - **Subred de nube**
   - **Grupo de ubicación en la nube** (esta unidad se muestra solamente si la instancia pertenece a un grupo de ubicación)

   Para los dispositivos en Azure, se muestran las siguientes propiedades:

   - **Dispositivo encontrado mediante API** (valor: **Microsoft Azure**)
   - **Región de la nube**
   - **Subred de nube**

   Para los dispositivos en Google Cloud, se muestran las siguientes propiedades:

   - **Dispositivo encontrado mediante API** (valor: **Google Cloud**)
   - **Región de la nube**
   - **Cloud VPC**
   - **Zona de disponibilidad en la nube**
   - **Subred de nube**

# Sincronización con la nube: Configuración de la regla de movimiento

Durante el funcionamiento de Configuración del entorno de nube, se crea la regla llamada Sincronizar con la nube de manera automática. La regla permite mover automáticamente los dispositivos detectados en cada sondeo del grupo "Dispositivos no asignados" al grupo "Dispositivos administrados\Cloud" para que se los pueda administrar en forma centralizada. De manera predeterminada, una vez que se crea esta regla, se la deja habilitada. Puede deshabilitar, modificar o aplicar la regla en cualquier momento.

*Para aplicar la regla "Sincronizar con la nube" o modificar sus propiedades:*

1. En el menú principal, vaya a **Descubrimiento y despliegue → Despliegue y asignación → Reglas de movimiento**.

   Se abre la lista de reglas de movimiento.

2. En la lista de reglas de movimiento, seleccione **Sincronizar con la nube**.

   Se abre la ventana de propiedades de la regla.

3. De ser necesario, configure los siguientes ajustes en la pestaña **Segmentos de nube** de la pestaña **Condiciones de la regla**:

- **El dispositivo se encuentra en un segmento de la nube**

  La regla solo se aplicará a los dispositivos que se encuentren en el segmento de nube seleccionado. De lo contrario, la regla se aplicará a todos los dispositivos que hayan sido detectados.

  Esta opción está seleccionada de forma predeterminada.

- **Incluir objetos secundarios**

  La regla se aplicará a todos los dispositivos del segmento seleccionado y a todas las subsecciones de nube anidadas. De lo contrario, la regla solo se aplicará a los dispositivos que estén en el segmento raíz.

  Esta opción está seleccionada de forma predeterminada.

- **Mover los dispositivos de objetos anidados a subgrupos correspondientes**

  Si esta opción está habilitada, los dispositivos de los objetos anidados se moverán automáticamente a los subgrupos que se correspondan con su estructura.

  Si esta opción está deshabilitada, los dispositivos de los objetos anidados se moverán automáticamente a la raíz del subgrupo "Cloud" y no habrá más ramificaciones.

  Esta opción está activada de forma predeterminada.

- **Crear subgrupos correspondientes a contenedores de dispositivos recién detectados**

  Si esta opción está habilitada, cuando la estructura de **Dispositivos administrados\Nube** no tiene subgrupos que coincidan con la sección que contiene el dispositivo, Kaspersky Security Center crea tales subgrupos. Por ejemplo, si se detecta una nueva subred durante el descubrimiento de dispositivos, se creará un nuevo grupo con el mismo nombre en el grupo **Dispositivos administrados\Cloud**.

  Si esta opción está desactivada, Kaspersky Security Center no crea ningún subgrupo nuevo. Si se descubre una nueva subred al sondear la red, por ejemplo, no se creará un nuevo grupo con el mismo nombre en el grupo **Dispositivos administrados\Cloud**, y los dispositivos que se encuentren en la subred detectada se moverán al grupo **Dispositivos administrados\Cloud**.

  Esta opción está activada de forma predeterminada.

- **Eliminar subgrupos para los que no se encuentre coincidencia en los segmentos de nube**

  Si esta opción está habilitada, la aplicación eliminará del grupo "Cloud" todo subgrupo que no tenga contraparte en un objeto de nube existente.

  Si esta opción está deshabilitada, se conservarán los subgrupos que no tengan contraparte en un objeto de nube existente.

  Esta opción está activada de forma predeterminada.

Si habilitó la opción **Sincronizar los grupos de administración con la estructura de nube** al utilizar Configuración del entorno de nube, la regla **Sincronizar con la nube** ya tendrá habilitadas las opciones **Crear subgrupos correspondientes a contenedores de dispositivos recién detectados** y **Eliminar subgrupos para los que no se encuentre coincidencia en los segmentos de nube**.

Si no habilitó la opción **Sincronizar los grupos de administración con la estructura de nube**, la regla **Sincronizar con la nube** no tendrá estas opciones habilitadas. Si, por el modo en que usted utiliza Kaspersky Security Center, necesita que la estructura de subgrupos dentro del subgrupo **Dispositivos administrados\Cloud** coincida con la estructura de los segmentos de nube, habilite las opciones **Crear subgrupos correspondientes a contenedores de dispositivos recién detectados** y **Eliminar subgrupos para los que no se encuentre coincidencia en los segmentos de nube** en las propiedades de la regla y aplique la regla.

4. En la lista desplegable **Dispositivo encontrado mediante API**, seleccione uno de los siguientes valores:

   - **No**. El dispositivo no puede detectarse usando las API de AWS, Azure o Google; es decir, o bien el dispositivo no forma parte del entorno de nube, o bien está en el entorno de nube, pero, por algún motivo, no se lo puede detectar a través de una de las API.
   - **AWS**. El dispositivo puede detectarse mediante la API de AWS, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de AWS.
   - **Azure**. El dispositivo puede detectarse mediante la API de Azure, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de Azure.
   - **Google Cloud**. El dispositivo puede detectarse mediante la API de Google, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de Google.
   - Ningún valor. Este criterio no se puede aplicar.

5. Si es necesario, configure las propiedades de la regla en las demás secciones.

La regla de movimiento queda configurada.

# Instalación remota de aplicaciones en máquinas virtuales de Azure

Para instalar aplicaciones en máquinas virtuales de Microsoft Azure, debe tener una licencia válida.

Kaspersky Security Center admite los siguientes escenarios:

- El dispositivo cliente se descubre a través de la API de Azure y la instalación se realiza, también, a través de una API. El uso de la API de Azure significa que solo puede instalar las siguientes aplicaciones:
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security para Windows
  - Kaspersky Security for Windows Server
- El dispositivo cliente se descubre a través de la API de Azure y la instalación se realiza a través de un punto de distribución o, si no hay puntos de distribución disponibles, de manera manual, utilizando paquetes de instalación independientes. Este método sirve para instalar cualquier aplicación compatible con Kaspersky Security Center Cloud Console.

*Para instalar una aplicación de forma remota en una máquina virtual de Azure, cree una tarea de este modo:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea.
3. Siga las instrucciones del asistente:

   a. Seleccione **Instalar aplicación de forma remota** como tipo de tarea.

   b. En la página **Paquetes de instalación**, seleccione **Instalación remota mediante Microsoft Azure API**.

   c. Al momento de seleccionar la cuenta con la que se accederá a los dispositivos, use una cuenta de Azure existente o haga clic en **Agregar** e ingrese las credenciales de su cuenta de Azure:

   - **Nombre de la cuenta de Azure**

     Escriba un nombre cualquiera para las credenciales que está introduciendo. El nombre aparecerá en la lista de cuentas para ejecutar la tarea.

   - **Id. de la aplicación en Azure**

     Usted creó el id. de la aplicación en el portal de Azure.

     No puede especificar más de un id. de aplicación de Azure para realizar sondeos u otros fines. Si desea sondear otro segmento de Azure, elimine primero la conexión de Azure existente.

   - **Contraseña de la aplicación en Azure**

     Recibió la contraseña correspondiente al id. de aplicación cuando creó dicho id.

     Los caracteres de la contraseña se muestran como asteriscos. Cuando empiece a introducir la contraseña, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado para ver los caracteres introducidos.

   d. Seleccione los dispositivos pertinentes en el grupo **Dispositivos administrados\Cloud**.

Cuando finalice el asistente, encontrará la tarea para instalar la aplicación en forma remota dentro de la lista de tareas.

# Creación de copia de seguridad de los datos del Servidor de administración en un DBMS en la nube

Las tareas de copia de seguridad son tareas del Servidor de administración. Puede crear una tarea de copia de seguridad si desea usar un DBMS alojado en un entorno de nube (AWS o Azure).

Para crear una tarea de copia de seguridad de los datos del Servidor de administración:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea.

3. En la primera página del asistente, en la lista **Aplicación**, seleccione **Kaspersky Security Center 15.1**. A continuación, en la lista **Tipo de tarea**, seleccione **Copia de seguridad de los datos del Servidor de administración**.

4. Cuando el asistente se lo solicite, introduzca la siguiente información:

   - Si la base de datos está alojada en AWS:

     - **Nombre del bucket de S3**

       El nombre del bucket de S3 que creó para la copia de seguridad.

     - **Id. de clave de acceso**

       Recibió el id. de clave (secuencia de caracteres alfanuméricos) cuando creó la cuenta de usuario de IAM para trabajar con la instancia de almacenamiento en buckets de S3.

       El campo está disponible si ha seleccionado la base de datos de RDS en un bucket de S3.

     - **Clave secreta**

       La clave secreta que recibió con el id. de la clave de acceso al crear la cuenta de usuario de IAM.

       Los caracteres de la clave secreta se muestran como asteriscos. Cuando comience a escribir la clave secreta, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado el tiempo que necesite para ver los caracteres introducidos.

       El campo está disponible si seleccionó una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

   - Si la base de datos está alojada en Microsoft Azure:

     - **Nombre de la cuenta de almacenamiento de Azure**

       Usted creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

     - **Id. de suscripción de Azure**

       Creó esta suscripción en el portal de Azure.

     - **Contraseña de Azure**

       Recibió la contraseña correspondiente al id. de aplicación cuando creó dicho id.

       Los caracteres de la contraseña se muestran como asteriscos. Cuando empiece a introducir la contraseña, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado para ver los caracteres introducidos.

     - **Id. de la aplicación en Azure**

Usted creó el id. de la aplicación en el portal de Azure.

No puede especificar más de un id. de aplicación de Azure para realizar sondeos u otros fines. Si desea sondear otro segmento de Azure, elimine primero la conexión de Azure existente.

- **Nombre del servidor SQL de Azure**

  El nombre y el grupo de recursos están disponibles en las propiedades del Servidor SQL de Azure.

- **Grupo de recursos del servidor SQL de Azure**

  El nombre y el grupo de recursos están disponibles en las propiedades del Servidor SQL de Azure.

- **Clave de acceso al almacenamiento de Azure**

  Disponible en las propiedades de su cuenta de almacenamiento, en la sección Claves de acceso. Puede utilizar cualquiera de las claves (key1 o key2).

Se crea la tarea y se la agrega a la lista de tareas. Si habilita la opción **Abrir los detalles de la tarea cuando se complete la creación**, podrá modificar la configuración predeterminada de la tarea en cuanto se la haya creado. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.

# Diagnóstico remoto de dispositivos cliente

Puede usar la función de diagnóstico remoto para realizar a distancia las siguientes operaciones en dispositivos cliente basados en Windows y Linux:

- Habilitar y deshabilitar la característica de seguimiento, cambiar el nivel de seguimiento y descargar el archivo de seguimiento
- Descargar información del sistema y los ajustes de las aplicaciones
- Descargar registros de eventos
- Crear un archivo de volcado para una aplicación
- Realizar un diagnóstico y descargar el informe de diagnóstico
- Iniciar, detener y reiniciar aplicaciones

Puede utilizar los registros de eventos y los informes de diagnóstico descargados de un dispositivo cliente para solucionar problemas por cuenta propia. Si se comunica con el servicio de soporte técnico de Kaspersky, los especialistas podrían pedirle que descargue archivos de seguimiento, archivos de volcado, registros de eventos e informes de diagnóstico del dispositivo cliente para que sean analizados en Kaspersky.

# Abrir la ventana de diagnóstico remoto

Para realizar un diagnóstico remoto de dispositivos cliente basados en Windows y Linux, debe abrir la ventana de diagnóstico remoto.

*Para abrir la ventana de diagnóstico remoto:*

1. Realice una de las siguientes acciones para seleccionar el dispositivo para el que desee abrir la ventana de diagnóstico remoto:

   - Si el dispositivo pertenece a un grupo de administración, en el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.

   - Si el dispositivo pertenece al grupo Dispositivos no asignados, en el menú principal, vaya a **Descubrimiento y despliegue** → **Dispositivos no asignados**.

2. Haga clic en el nombre del dispositivo pertinente.

3. En la ventana que se abre, que contendrá las propiedades del dispositivo, elija la pestaña **Avanzado**.

4. En la ventana que se abre, haga clic en **Diagnóstico remoto**.

   Esto abre la ventana **Diagnóstico remoto** de un dispositivo cliente. Si no se establece la conexión entre el Servidor de administración y el dispositivo cliente, se muestra el mensaje de error.

Como alternativa, si necesita obtener toda la información de diagnóstico sobre un dispositivo cliente basado en Linux a la vez, puede ejecutar el script collect.sh en este dispositivo.

# Habilitar y deshabilitar el seguimiento para las aplicaciones

Puede habilitar y deshabilitar el seguimiento para las aplicaciones, incluido el seguimiento con Xperf.

## Habilitar y deshabilitar el seguimiento

*Para habilitar o deshabilitar el seguimiento en un dispositivo remoto:*

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.

2. En la ventana de diagnóstico remoto, seleccione la pestaña **Aplicaciones de Kaspersky**.

   En la sección **Administración de aplicaciones**, se muestra la lista de aplicaciones de Kaspersky instaladas en el dispositivo.

3. En la lista de aplicaciones, seleccione la aplicación para la que desee habilitar o deshabilitar el seguimiento.

   Se abre la lista de opciones de diagnóstico remoto.

4. Si desea habilitar el seguimiento, haga lo siguiente:

   a. En la sección **Seguimiento**, haga clic en **Habilitar seguimiento**.

   b. En la ventana **Modificar nivel de seguimiento**, recomendamos que mantenga los valores de configuración predeterminados. De ser necesario, un especialista del servicio de soporte técnico le indicará cómo modificar la configuración. Las opciones de configuración disponibles son las siguientes:

   - Nivel de seguimiento

     El nivel de seguimiento determina qué tan detallado es el archivo de seguimiento.

   - Seguimiento con rotación

     La información de seguimiento se sobrescribe para que el archivo de seguimiento no aumente de tamaño desmedidamente. Especifique el número máximo de archivos que se utilizarán para almacenar la información de seguimiento y el tamaño máximo de cada archivo. Una vez que se haya guardado el número máximo de archivos de seguimiento, cada cual con su tamaño máximo, se eliminará el archivo de seguimiento más antiguo para que se pueda guardar un nuevo archivo de seguimiento.

     Esta opción solo está disponible para Kaspersky Endpoint Security.

   c. Haga clic en **Guardar**.

   Se habilita el seguimiento para la aplicación seleccionada. En algunos casos, para habilitar el seguimiento, deberá reiniciar la aplicación de seguridad y su tarea.

   En dispositivos cliente basados en Linux, el seguimiento del componente Actualizador del Agente de red está regulado por la configuración del Agente de red. Por lo tanto, las opciones **Habilitar seguimiento** y **Modificar nivel de seguimiento** están deshabilitadas para este componente en dispositivos cliente que ejecutan Linux.

5. Para deshabilitar el seguimiento para la aplicación seleccionada, haga clic en el botón **Deshabilitar seguimiento**.

   Se deshabilita el seguimiento para la aplicación seleccionada.

## Habilitar el seguimiento con Xperf

Si utiliza Kaspersky Endpoint Security, un especialista de nuestro servicio de soporte técnico podría pedirle que habilite el seguimiento con Xperf. Esta función permite obtener información sobre el rendimiento del sistema.

*Para habilitar y configurar el seguimiento con Xperf o deshabilitarlo, siga los siguientes pasos:*

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.

2. En la ventana de diagnóstico remoto, seleccione la pestaña **Aplicaciones de Kaspersky**.

   En la sección **Administración de aplicaciones**, se muestra la lista de aplicaciones de Kaspersky instaladas en el dispositivo.

3. En la lista de aplicaciones, seleccione Kaspersky Endpoint Security para Windows.

   Se muestra la lista de opciones de diagnóstico remoto para la app Kaspersky Endpoint Security para Windows.

4. En la sección **Seguimiento con Xperf**, haga clic en **Habilitar seguimiento con Xperf**.

   Si el seguimiento con Xperf ya está habilitado, verá, en cambio, el botón **Deshabilitar seguimiento con Xperf**. Haga clic en este botón si desea deshabilitar el seguimiento con Xperf para Kaspersky Endpoint Security para Windows.

5. Cuando se abra la ventana **Cambiar el nivel de seguimiento con Xperf**, dependiendo de lo que le haya pedido el especialista en soporte técnico, haga lo siguiente:

   a. Seleccione uno de los siguientes niveles de seguimiento:

   - **Nivel bajo**

     Un archivo de seguimiento de este tipo contiene una cantidad mínima de información sobre el sistema.

     Esta opción está seleccionada de forma predeterminada.

   - **Nivel profundo**

     Un archivo de seguimiento de este tipo contiene información más detallada que los archivos de seguimiento que se generan cuando se elige la opción *Nivel bajo*. El especialista en soporte técnico podría pedirle que elija este nivel si la información contenida en un archivo de nivel bajo no basta para evaluar el rendimiento del sistema. Un archivo de seguimiento de *Nivel profundo* contiene distintas clases de información técnica sobre el sistema: información sobre el hardware, el sistema operativo, la lista de procesos y programas iniciados y finalizados, los eventos utilizados para la evaluación del rendimiento, eventos de la Herramienta de evaluación del sistema de Windows y más.

   b. Seleccione uno de los siguientes tipos de seguimiento con Xperf:

   - **Tipo básico**

     La información de seguimiento se obtendrá mientras Kaspersky Endpoint Security esté en funcionamiento.

     Esta opción está seleccionada de forma predeterminada.

   - **Tipo con reinicio**

     La información de seguimiento se obtendrá cuando se inicie el sistema operativo del dispositivo administrado. Este tipo de seguimiento es efectivo cuando el problema que afecta al rendimiento del sistema ocurre después de encender el dispositivo y antes de que se inicie Kaspersky Endpoint Security.

   También podrían pedirle que habilite la opción **Tamaño de archivos de rotación, en MB** para evitar que el archivo de seguimiento aumente de tamaño desmedidamente. Si habilita esta opción, especifique el tamaño que el archivo de seguimiento podrá tener como máximo. Cuando el archivo alcance su máximo tamaño, la información de seguimiento más antigua comenzará a reemplazarse con información nueva.

   c. Defina el tamaño del archivo de rotación.

   d. Haga clic en **Guardar**.

   El seguimiento con Xperf queda configurado y habilitado.

6. Si desea deshabilitar el seguimiento con Xperf para Kaspersky Endpoint Security para Windows, haga clic en **Deshabilitar seguimiento con Xperf** en la sección **Seguimiento con Xperf**.

   Se deshabilita el seguimiento con Xperf.

# Descargar los archivos de seguimiento de una aplicación

*Para descargar un archivo de seguimiento de una aplicación:*

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, seleccione la pestaña **Aplicaciones de Kaspersky**.

   En la sección **Administración de aplicaciones**, se muestra la lista de aplicaciones de Kaspersky instaladas en el dispositivo.
3. En la lista de aplicaciones, seleccione la aplicación para la que desee descargar un archivo de seguimiento.
4. En la sección **Seguimiento**, haga clic en el botón **Archivos de seguimiento**.

   Se abre la ventana **Registros de seguimiento del dispositivo**, en la que se muestra una lista de archivos de seguimiento.
5. En la lista de archivos de seguimiento, seleccione el archivo que desee descargar.
6. Realice una de las siguientes acciones:

   - Si desea descargar el archivo seleccionado, haga clic en **Descargar**. Puede seleccionar uno o varios archivos para descargar.
   - Si desea descargar una parte del archivo seleccionado, haga lo siguiente:

     a. Haga clic en **Descargar una parte**.

     No puede descargar partes de varios archivos al mismo tiempo. Si selecciona más de un archivo de seguimiento, se deshabilita el botón **Descargar una parte**.

     b. En la ventana que se abre, indique el nombre y la parte del archivo que desee descargar.

     Para dispositivos basados en Linux, no está disponible la edición del nombre de la parte del archivo.

     c. Haga clic en **Descargar**.

El archivo seleccionado, o la parte seleccionada, se descargará en la ubicación que especifique.

# Eliminar archivos de seguimiento

Puede eliminar los archivos de seguimiento que ya no necesite.

*Para eliminar un archivo de seguimiento:*

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto que se abre, seleccione la pestaña **Registros de eventos**.

3. En la sección **Archivos de seguimiento**, haga clic en **Registros de Windows Update** o en **Registros de instalación remota**, dependiendo de cuáles sean los archivos de seguimiento que desee eliminar.

   El vínculo **Registros de Windows Update** está disponible solo para dispositivos cliente basados en Windows.

   Se abre la ventana **Registros de seguimiento del dispositivo**, en la que se muestra una lista de archivos de seguimiento.

4. En la lista de archivos de seguimiento, seleccione uno o varios archivos que desee eliminar.

5. Haga clic en el botón **Eliminar**.

Los archivo de seguimiento seleccionados se eliminan.

# Descargar la configuración de las aplicaciones

*Para descargar la configuración de las aplicaciones instaladas en un dispositivo cliente:*

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.

2. En la ventana de diagnóstico remoto, seleccione la pestaña **Aplicaciones de Kaspersky**.

3. En la sección **Configuración de las aplicaciones**, haga clic en el botón **Descargar** para descargar la información sobre la configuración de las aplicaciones instaladas en el dispositivo cliente.

En la ubicación especificada, se descarga el archivo ZIP con la información.

# Descargar registros de eventos

*Para descargar un registro de eventos de un dispositivo remoto:*

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.

2. En la ventana de diagnóstico remoto, en la pestaña **Registros de eventos**, haga clic en **Todos los registros del dispositivo**.

3. En la ventana **Todos los registros del dispositivo**, seleccione uno o varios registros que desee descargar.

4. Realice una de las siguientes acciones:

   - Si desea descargar el archivo de registro seleccionado, haga clic en **Descargar archivo completo**.

   - Si desea descargar una parte del archivo de registro seleccionado, haga lo siguiente:

     a. Haga clic en **Descargar una parte**.

     No puede descargar partes de varios registros al mismo tiempo. Si selecciona más de un registro de eventos, se deshabilita el botón **Descargar una parte**.

     b. En la ventana que se abre, indique el nombre y la parte del registro que desee descargar.

     Para dispositivos basados en Linux, no está disponible la edición del nombre del registro.

     c. Haga clic en **Descargar**.

El registro de eventos seleccionado, o la parte seleccionada, se descarga en la ubicación especificada.

# Iniciar, detener o reiniciar la aplicación

Puede iniciar, detener y reiniciar las aplicaciones instaladas en los dispositivos cliente.

*Para iniciar, detener o reiniciar una aplicación:*

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.

2. En la ventana de diagnóstico remoto, seleccione la pestaña **Aplicaciones de Kaspersky**.

   En la sección **Administración de aplicaciones**, se muestra la lista de aplicaciones de Kaspersky instaladas en el dispositivo.

3. En la lista de aplicaciones, seleccione la aplicación que desee iniciar, detener o reiniciar.

4. Haga clic en uno de los siguientes botones para realizar la acción correspondiente:

   - **Detener la aplicación**

     Este botón solo estará disponible si la aplicación se encuentra en ejecución.

   - **Reiniciar aplicación**

     Este botón solo estará disponible si la aplicación se encuentra en ejecución.

   - **Iniciar la aplicación**

     Este botón solo estará disponible si la aplicación no se encuentra en ejecución.

   Dependiendo de la acción que haya elegido, la aplicación seleccionada se iniciará, se detendrá o se reiniciará en el dispositivo cliente.

Si elige reiniciar el Agente de red, se le advertirá que la conexión entre el dispositivo y el Servidor de administración se cerrará.

# Realizar un diagnóstico remoto del Agente de red de Kaspersky Security Center y descargar los resultados

*Para realizar un diagnóstico del Agente de red de Kaspersky Security Center en un dispositivo remoto y descargar los resultados:*

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, seleccione la pestaña **Aplicaciones de Kaspersky**.

   En la sección **Administración de aplicaciones**, se muestra la lista de aplicaciones de Kaspersky instaladas en el dispositivo.
3. En la lista de aplicaciones, seleccione **Agente de red de Kaspersky Security Center**.

   Se abre la lista de opciones de diagnóstico remoto.
4. En la sección **Informe de diagnóstico**, haga clic en el botón **Ejecutar diagnóstico**.

   Se iniciará el proceso de diagnóstico remoto y se generará un informe con el resultado. Cuando se complete el proceso, la aplicación le permitirá hacer clic en el botón **Descargar informe de diagnóstico**.
5. Haga clic en el botón **Descargar informe de diagnóstico** para descargar el informe.

En la ubicación especificada, se descarga el archivo.

# Ejecutar una aplicación en un dispositivo cliente

Ocasionalmente, un especialista del Soporte técnico de Kaspersky puede pedirle que ejecute una aplicación en el dispositivo cliente. Si esto sucede, no es necesario que instale la aplicación en el dispositivo cliente.

*Para ejecutar una aplicación en un dispositivo cliente:*

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, seleccione la pestaña **Ejecución de una aplicación remota**.
3. En la sección **Archivos de aplicación**, haga clic en el botón **Examinar** para seleccionar un archivo ZIP que contenga la aplicación que desea ejecutar en el dispositivo cliente.

   > El archivo ZIP debe incluir la carpeta de la utilidad. Esta carpeta contiene el archivo ejecutable que se ejecuta en un dispositivo remoto.

   Puede especificar el nombre del archivo ejecutable y los argumentos de la línea de comandos, si es necesario. Para hacer esto, complete los campos **Archivo ejecutable en un archivo para ejecutarse en un dispositivo remoto** y **Argumentos para la línea de comandos**.
4. Haga clic en el botón **Cargar y ejecutar** para ejecutar la aplicación especificada en un dispositivo cliente.
5. Siga las instrucciones del especialista del Servicio de soporte técnico de Kaspersky.

# Crear un archivo de volcado para una aplicación

El archivo de volcado de una aplicación le permite ver los parámetros de la aplicación que se ejecuta en un dispositivo cliente en un momento determinado. Este archivo también contiene información sobre los módulos que se cargaron para una aplicación.

No se admite la obtención de archivos de volcado de dispositivos con Linux.

Para obtener archivos de volcado mediante diagnósticos remotos, se utiliza la utilidad kldumper. Esta utilidad está diseñada para recopilar los archivos de volcado de procesos de aplicaciones de Kaspersky a pedido de los especialistas del servicio de soporte técnico. Puede encontrar información detallada sobre los requisitos para usar la utilidad kldumper en la Base de conocimientos de Kaspersky Security Center.

*Si desea crear un archivo de volcado para una aplicación:*

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, seleccione la pestaña **Ejecución de una aplicación remota**.
3. En la sección **Generación de un volcado de memoria del proceso**, especifique el archivo ejecutable de la aplicación para la que desea generar un archivo de volcado.
4. Haga clic en el botón **Descargar archivo de volcado**.

   Se descargará un archivo de volcado de la aplicación especificada.

   Si la aplicación especificada no se está ejecutando en el dispositivo cliente, la carpeta "result" en el archivo descargado estará vacía.

   Si la aplicación especificada se está ejecutando, pero la descarga falla por un error o la carpeta "result" en el archivo descargado está vacía, consulte la Base de conocimientos de Kaspersky Security Center.

# Ejecución de diagnósticos remotos en un dispositivo cliente basado en Linux

Kaspersky Security Center le permite descargar la información de diagnóstico básica desde un dispositivo cliente. Como alternativa, puede obtener información de diagnóstico sobre un dispositivo basado en Linux utilizando el script collect.sh de Kaspersky. Este script se ejecuta en el dispositivo cliente basado en Linux que necesita ser diagnosticado y luego genera un archivo con la información de diagnóstico, la información del sistema sobre este dispositivo, archivos de seguimiento de aplicaciones, registros del dispositivo y un archivo de volcado para emergencias. aplicaciones terminadas.

Le recomendamos que utilice el script collect.sh para obtener toda la información de diagnóstico sobre el dispositivo cliente basado en Linux a la vez. Si descarga la información de diagnóstico de forma remota a través de Kaspersky Security Center, deberá revisar todas las secciones de la interfaz de diagnóstico remoto. Además, es probable que la información de diagnóstico de un dispositivo basado en Linux no se obtenga por completo.

Si necesita enviar el archivo generado con la información de diagnóstico al Servicio de soporte técnico de Kaspersky, elimine toda la información confidencial antes de enviar el archivo.

*Para descargar la información de diagnóstico desde un dispositivo cliente basado en Linux mediante el script collect.sh:*

1. Descargue el script collect.sh comprimido en el archivo collect.tar.gz.
2. Copie el archivo descargado en el dispositivo cliente basado en Linux que necesita ser diagnosticado.
3. Ejecute el siguiente comando para descomprimir el archivo collect.tar.gz:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Ejecute el siguiente comando para especificar los derechos de ejecución del script:

   ```
   # chmod +x collect.sh
   ```

5. Ejecute el script collect.sh utilizando una cuenta con derechos de administrador:

   ```
   # ./collect.sh
   ```

Se genera un archivo con la información de diagnóstico y se guarda en la carpeta /tmp/$HOST_NAME-collect.tar.gz.

# Descarga y eliminación de archivos de Cuarentena y Copia de seguridad

Esta sección brinda información sobre cómo descargar y eliminar archivos de Cuarentena y Copia de seguridad en Kaspersky Security Center Web Console.

## Descarga de archivos de Cuarentena y Copia de seguridad

Los archivos almacenados en Cuarentena y en Copia de seguridad pueden descargarse si la opción **No desconectar del Servidor de administración** está habilitada en la configuración del dispositivo o si se está utilizando una puerta de enlace de conexión. Si no se cumple ninguna de estas condiciones, no podrá realizar la descarga.

*Para guardar en el disco duro una copia de un archivo almacenado en Cuarentena o en Copia de seguridad:*

1. Realice una de las siguientes acciones:

   - Si desea guardar una copia de un archivo que se encuentra en Cuarentena, en el menú principal vaya a **Operaciones → Repositorios → Cuarentena**.

   - Si desea guardar una copia de un archivo que se encuentra en Copia de seguridad, en el menú principal vaya a **Operaciones → Repositorios → Copia de seguridad**.

2. En la ventana que se abre, seleccione el archivo que desea descargar y haga clic en **Descargar**.

   Comienza la descarga. La aplicación guarda, en la carpeta seleccionada, una copia del archivo almacenado en el repositorio Cuarentena del dispositivo cliente.

# Cambiar el idioma de la interfaz de Kaspersky Security Center Web Console

Puede seleccionar el idioma de la interfaz de Kaspersky Security Center Web Console.

*Para cambiar el idioma de la interfaz, haga lo siguiente:*

1. En el menú principal, vaya a **Configuración → Idioma**.

2. Seleccione uno de los idiomas de localización admitidos.

# Guía de referencia de API

Esta guía de referencia de OpenAPI de Kaspersky Security Center está diseñada para ayudar en las siguientes tareas:

- Automatización y personalización. Puede automatizar las tareas que no quiera manejar manualmente utilizando la Consola de administración. También puede implementar escenarios personalizados que aún no son compatibles con la Consola de administración. Por ejemplo, como administrador, puede utilizar OpenAPI de Kaspersky Security Center para crear y ejecutar scripts que faciliten el desarrollo de la estructura de los grupos de administración y mantengan dicha estructura actualizada.

- Desarrollo personalizado. Por ejemplo, puede desarrollar una Consola de administración basada en MMC alternativa para sus clientes, que permita un conjunto limitado de acciones.

Para encontrar la información que necesita en la guía de referencia de OpenAPI, puede utilizar el campo de búsqueda ubicado en la parte derecha de la pantalla.

GUÍA DE REFERENCIA DE OPENAPI

## Muestras de scripts

La guía de referencia de OpenAPI contiene muestras de los scripts de Python que se enumeran en la siguiente tabla. Los ejemplos muestran cómo puede llamar a métodos OpenAPI y realizar automáticamente varias tareas para proteger su red, por ejemplo, crear una jerarquía "primario/secundario", ejecutar tareas en Kaspersky Security Center, o asignar puntos de distribución. Puede ejecutar los ejemplos o crear sus propios scripts basados en los ejemplos.

*Para llamar a los métodos OpenAPI y ejecutar scripts:*

1. Descargue el archivo KlAkOAPI.tar.gz. Este archivo incluye el paquete KlAkOAPI y las muestras (puede copiarlas del archivo o de la guía de referencia de OpenAPI). El archivo KlAkOAPI.tar.gz también se encuentra en la carpeta de instalación de Kaspersky Security Center.

2. Instale el paquete KlAkOAPI del archivo KlAkOAPI.tar.gz en un dispositivo donde esté instalado el Servidor de administración.

   Puede llamar a los métodos de OpenAPI, ejecutar las muestras y sus propios scripts solo en dispositivos donde estén instalados el Servidor de administración y el paquete KlAkOAPI.

Coincidencia entre procedimientos de usuario y ejemplos de métodos OpenAPI de Kaspersky Security Center

| Ejemplo | Propuesta del ejemplo | Procedimiento |
|---|---|---|
| Registro KlAkParams | Puede extraer y procesar datos usando la estructura de datos `KlAkParams`. La muestra indica cómo trabajar con esta estructura de datos.<br>La salida de la muestra se puede presentar de diferentes maneras. Puede obtener los datos para enviar un método HTTP o para usarlo en su código. | Supervisión e informes |
| Crear y eliminar una jerarquía "principal/secundario" | Puede agregar un Servidor de administración secundario para establecer una jerarquía "principal/secundario". Alternativamente, puede desconectar de la jerarquía el Servidor de administración secundario. | • Creación de una jerarquía de servidores de administración: agregar un Servidor de administración secundario<br>• Eliminar una jerarquía de servidores de administración |
| Crear la jerarquía de grupo con una estructura basada en la unidad de Active Directory | Puede sondear la unidad de Active Directory y formar una jerarquía de grupos con los dispositivos descubiertos. | Creación de grupos de administración |
| Crear la jerarquía de grupo con una estructura basada en la unidad de Active Directory en caché | Puede formar una jerarquía de los grupos de dispositivos administrados en función de la unidad de Active Directory sondeada anteriormente. Si después del último sonde aparecen nuevos dispositivos en el directorio activo, no se los añade al grupo porque no están en los resultados de sondeo guardados. | Creación de grupos de administración |
| Descargar archivos con listas de redes a un dispositivo específico mediante la puerta de enlace de conexión | Puede conectarse al agente de red en el dispositivo necesario utilizando una pasarela de conexión y luego descargar un archivo con la lista de red a su dispositivo. | Ajuste de puntos de distribución y puertas de enlace de conexión |
| Instalar una clave de licencia almacenada en el repositorio del Servidor de administración principal en los servidores de administración secundarios | Puede conectarse al Servidor de administración principal, descargar desde allí la clave de licencia necesaria y transmitirla a todos los Servidores de administración secundarios incluidos en una jerarquía. | Licencias de aplicaciones administradas |
| Crear un informe de derechos de usuario efectivos | Puede crear diferentes informes Por ejemplo, puede generar el informe de derechos de usuario efectivos utilizando esta muestra. Este informe describe los derechos que tiene un usuario, dependiendo de su grupo y papel.<br>Puede descargar el informe en formato HTML, PDF o Excel. | Generar y ver un informe |
| Iniciar una tarea para un dispositivo | Puede conectarse al Agente de red en el dispositivo necesario utilizando una pasarela de conexión y luego ejecutar la tarea necesaria. | Iniciar una tarea manualmente |

| Ejemplo | Propuesta del ejemplo | Procedimiento |
| --- | --- | --- |
| Crear subredes IP basadas en el sitio y los servicios de Active Directory | Puede crear una subred IP según la unidad de Active Directory que use.<br><br>La muestra inicia el sondeo del rango de IP especificado y elimina las subredes descubiertas para impedir que entren en conflicto con una nueva subred. Por lo tanto, no ejecute esta muestra en la red donde sea importante mantener las subredes.<br><br>Después de realizar el sondeo, la muestra recurre a Active Directory, examina cada dispositivo en él y crea la subred IP. Para ello, la muestra utiliza las máscaras y las direcciones IP de todos los dispositivos. | Configurar la protección de la red |
| Registrar puntos de distribución para los dispositivos de un grupo | Puede asignar dispositivos administrados como puntos de distribución (antes conocidos como agentes de actualización). | Actualización de las bases de datos y las aplicaciones de Kaspersky |
| Enumerar todos los grupos | Puede realizar varias acciones en los grupos de administración: El ejemplo muestra cómo hacer lo siguiente:<br><br>• Obtener un identificador del grupo raíz "Dispositivos administrados"<br>• Moverse a través de la jerarquía de grupo<br>• Recuperar la jerarquía completa y ampliada de los grupos, junto con sus nombres y nivel de anidación | Configuración del Servidor de administración |
| Enumerar las tareas, consultar las estadísticas de las tareas y ejecutar una tarea | Puede averiguar la siguiente información:<br><br>• Historial de progreso de la tarea<br>• Estado de la tarea actual<br>• Número de tareas en diferentes estados<br><br>También puedes ejecutar una tarea. De forma predeterminada, la muestra ejecuta una tarea después de emitir sus estadísticas. | Supervisar la ejecución de tareas |
| Crear y ejecutar una tarea | Puede crear una tarea Especifique los siguientes parámetros de la tarea en la muestra:<br><br>• Tipo<br>• Método de ejecución<br>• Nombre<br>• Grupo de dispositivos para el cual se utilizará la tarea<br><br>De forma predeterminada, la muestra crea una tarea con el tipo "Mostrar mensaje". Puede ejecutar esta tarea para todos los dispositivos administrados del Servidor de administración. Si es necesario, puede especificar sus propios parámetros de tarea. | Crear una tarea |
| Enumerar las claves de licencia | Puede obtener una lista de todas las claves de licencia activas para aplicaciones Kaspersky instaladas en dispositivos administrados de Administration Server. La lista contiene datos detallados sobre cada clave de licencia, como un nombre, tipo o fecha de vencimiento. | Visualización de información sobre las claves de licencia en uso |
| Crear y encontrar un usuario interno | Puede crear una cuenta para un trabajo adicional. | Seleccionar la cuenta para iniciar el Servidor de administración |
| Crear una categoría personalizada | Puede crear la categoría de aplicación con los parámetros necesarios. | Creación de una categoría de aplicaciones con contenido agregado manualmente |
| Enumerar los usuarios mediante SrvView | Puede usar la clase SrvView para solicitar información detallada al Servidor de administración. Por ejemplo, puede obtener una lista de usuarios utilizando esta muestra. | Administrar cuentas de usuario |

## Aplicaciones que interactúan con Kaspersky Security Center a través de OpenAPI

Algunas aplicaciones interactúan con Kaspersky Security Center a través de OpenAPI. Ejemplo de ellas son Kaspersky Anti Targeted Attack Platform y Kaspersky Security for Virtualization. También pueden ser aplicaciones cliente personalizadas, desarrolladas por usted para utilizar OpenAPI.

Las aplicaciones que interactúan con Kaspersky Security Center a través de OpenAPI se conectan al Servidor de administración. Si configuró una lista de direcciones IP autorizadas a conectarse al Servidor de administración, agregue las direcciones IP de los dispositivos en los que estén instaladas las aplicaciones que utilicen la interfaz OpenAPI de Kaspersky Security Center. Para saber si una aplicación utiliza OpenAPI, consulte la ayuda de esa aplicación.

# Prácticas recomendadas para proveedores de servicios

Esta sección proporciona información sobre cómo configurar y usar Kaspersky Security Center.

Esta sección contiene recomendaciones para instalar, configurar y usar la aplicación. También describe modos de resolver problemas habituales en el funcionamiento de la aplicación.

## Planificación de la distribución de Kaspersky Security Center

Al planear la distribución de los componentes de Kaspersky Security Center en una red de la organización, debe tener en cuenta el tamaño y el alcance del proyecto; específicamente, los siguientes factores:

- Número total de dispositivos.
- Número de clientes MSP.

Un Servidor de administración puede admitir un máximo de 100 000 dispositivos. Cuando el número total de dispositivos en la red de la organización supera los 100 000, hay que instalar varios Servidores de administración en la infraestructura del proveedor de servicios y combinarlos en una jerarquía para facilitar la administración centralizada.

Se pueden crear hasta 500 servidores virtuales en un solo Servidor de administración, por lo que se requiere un Servidor de administración particular por cada 500 clientes MSP.

En la etapa de planificación del despliegue, es necesario tener en cuenta la asignación del certificado especial X.509 al Servidor de administración. La asignación del certificado X.509 al Servidor de administración puede ser útil en los casos siguientes (lista parcial):

- Para la inspección del tráfico de la capa de sockets seguros (SSL) mediante un de terminación SSL
- Para especificar los valores requeridos de los campos del certificado
- Para proporcionar la solidez de cifrado deseada del certificado

## Suministro de acceso a Internet al Servidor de administración

Para permitir que los dispositivos en la red del cliente accedan al Servidor de administración mediante Internet, debe abrir los siguientes puertos del Servidor de administración:

- 13000 TCP: puerto TLS del Servidor de administración para conectar Agentes de red instalados en la red del cliente
- 8061 TCP: puerto HTTPS para publicar paquetes independientes usando herramientas de la Consola de administración

- 8060 TCP: puerto HTTP para publicar paquetes independientes usando herramientas de la Consola de administración

- 13292 TCP: puerto de TLS solo requerido si hay dispositivos móviles que se deban administrar

Si necesita proporcionar a los clientes opciones básicas de administración de red a través de Kaspersky Security Center Web Console, también debe abrir el puerto 8080 TCP (puerto HTTPS) de Kaspersky Security Center Web Console.

# Configuración estándar de Kaspersky Security Center

Uno o varios Servidores de administración están instalados en los servidores del MSP. El número de Servidores de administración puede seleccionarse según el hardware disponible, el número total de clientes MSP o el número total de dispositivos administrados.

Un Servidor de administración puede admitir un máximo de 100 000 dispositivos. Debe considerar la posibilidad de aumentar el número de dispositivos administrados en el futuro próximo: puede ser útil conectar un número levemente menor de dispositivos a un solo Servidor de administración.

Se pueden crear hasta 500 servidores virtuales en un solo Servidor de administración, por lo que se requiere un Servidor de administración particular por cada 500 clientes MSP.

Si se utilizan varios servidores, se recomienda que los combine en una jerarquía. La utilización de una jerarquía de Servidores de administración le permite evitar directivas y tareas duplicadas, gestionar el conjunto completo de dispositivos administrados, como si fueran administrados por un solo Servidor de administración; por ejemplo, buscar dispositivos, crear selecciones de dispositivos y crear informes.

En cada servidor virtual que corresponda a un cliente MSP, debe asignar uno o varios puntos de distribución. Si los clientes MSP y el Servidor de administración se vinculan por Internet, puede ser útil crear una tarea *Descargar actualizaciones a los repositorios de puntos de distribución* para los puntos de distribución, de modo que descarguen las actualizaciones directamente desde los servidores de Kaspersky, no desde el Servidor de administración.

Si algunos dispositivos en la red del cliente MSP no tienen acceso directo a Internet, debe cambiar los puntos de distribución al modo de puerta de enlace de conexión. En este caso, los Agentes de red en los dispositivos en la red del cliente MSP se conectarán, para mayor sincronización, al Servidor de administración, pero mediante la puerta de enlace, no de manera directa.

Dado que lo más probable es que el Servidor de administración no pueda sondear la red del cliente MSP, puede ser útil trasladar esta función a un punto de distribución.

El Servidor de administración no podrá enviar notificaciones al puerto UDP 15000 a dispositivos administrados ubicados detrás de la NAT en la red del cliente MSP. Para resolver este problema, puede ser útil activar el modo de conexión continua con el Servidor de administración en las propiedades de los dispositivos que funcionan como puntos de distribución y se ejecutan en el modo de Puerta de enlace de conexión (casilla **No desconectar del Servidor de administración**). El modo de conexión continua está disponible si el número total de puntos de distribución no supera los 300.

# Acerca de los puntos de distribución

Un dispositivo con el Agente de red instalado se puede utilizar como punto de distribución. En este modo, el Agente de red puede realizar las funciones siguientes:

- Transferir archivos a dispositivos cliente, incluidos:
  - Actualizaciones de las bases de datos y módulos de software de Kaspersky

    Las actualizaciones se pueden obtener desde el Servidor de administración o desde los servidores de actualización de Kaspersky. En este último caso, se debe crear *la tarea Descargar actualizaciones a los repositorios de puntos de distribución* para el dispositivo que sirve como punto de distribución.
  - Actualizaciones para el software de terceros
  - Paquetes de instalación
  - Actualizaciones de Windows si utiliza el Servidor de Administración como servidor WSUS
- Instalar software (incluido el Agente de red, durante el despliegue inicial) en otros dispositivos.
- Sondear la red para detectar nuevos dispositivos y actualizar la información disponible sobre los dispositivos de los que ya se tenía conocimiento. Un punto de distribución puede aplicar los mismos métodos de descubrimiento de dispositivos que el Servidor de administración.

Designar puntos de distribución en la red de una organización tiene los siguientes objetivos:

- Reducir la carga en el Servidor de administración si funciona como la fuente de actualizaciones.
- Optimizar el tráfico de Internet ya que, en este caso, no es necesario que cada dispositivo de la red del cliente MSP tenga acceso a servidores de Kaspersky o el Servidor de administración para descargar actualizaciones.
- Proporcionar al Servidor de administración acceso a dispositivos detrás de NAT (con relación al Servidor de administración) de la red del cliente MSP, lo que permite que el Servidor de administración realice las acciones siguientes:
  - Envíe notificaciones a dispositivos mediante UDP en la red IPv4 o IPv6.
  - Sondee la red IPv4 o IPv6.
  - Realizar el despliegue inicial.
  - Actúe como un servidor push.

Un punto de distribución se asigna a un grupo de administración. En este caso, el alcance del punto de distribución incluye todos los dispositivos dentro del grupo de administración y todos sus subgrupos. Sin embargo, el dispositivo que actúa como punto de distribución no se puede incluir en el grupo de administración al cual se ha asignado.

Puede hacer que un punto de distribución funcione como una puerta de enlace de conexión. En este caso, los dispositivos en el alcance del punto de distribución se conectarán al Servidor de administración a través de la puerta de enlace, no directamente. Puede usar este modo en situaciones que no permitan el establecimiento de una conexión directa entre dispositivos con el Agente de red y un Servidor de administración.

Los dispositivos designados como puntos de distribución deben protegerse contra el acceso no autorizado por medios virtuales y físicos.

# Jerarquía de Servidores de administración

Un MSP puede ejecutar varios Servidores de administración. Puede ser poco conveniente administrar varios Servidores de administración independientes, por lo que se puede aplicar una jerarquía. La configuración "principal/secundario" de dos Servidores de administración proporciona las opciones siguientes:

- Un Servidor de administración secundario hereda directivas y tareas del Servidor de administración principal. De esta forma se previene la duplicación de parámetros.
- Las selecciones de dispositivos en el Servidor de administración principal pueden incluir dispositivos desde los Servidores de administración secundarios.
- Los informes sobre el Servidor de administración principal pueden contener datos (incluida información detallada) de los Servidores de administración secundarios.

El Servidor de administración principal solo recibe datos de Servidores de administración secundarios no virtuales dentro del alcance de las opciones antes enumeradas. Esta limitación no se aplica a los Servidores de administración virtuales, que comparten la base de datos con su Servidor de administración principal.

# Servidores de administración virtuales

Sobre la base de un Servidor de administración físico, se pueden crear varios Servidores de administración virtual, los que serán similares a los Servidores de administración secundarios. En comparación con el modelo de acceso discrecional, que se basa en listas de control de acceso (ACL), el modelo del Servidor de administración virtual es más funcional y proporciona un mayor nivel de aislamiento. Además de una estructura dedicada de grupos de administración para dispositivos asignados con directivas y tareas, cada Servidor de administración virtual presenta su propio grupo de dispositivos no asignados, sus propios conjuntos de informes, dispositivos seleccionados y eventos, paquetes de instalación, reglas de traslado, etc. Para el aislamiento mutuo máximo de clientes MSP, recomendamos que elija Servidores de administración virtuales como la funcionalidad que se utilizará. Asimismo, la creación de un Servidor de administración virtual para cada cliente MSP le permite proporcionar a clientes opciones básicas de administración de la red mediante Kaspersky Security Center Web Console.

Los Servidores de administración virtual son muy similares a los Servidores de administración secundarios, pero con las distinciones siguientes:

- Un Servidor de administración virtual carece de la mayoría de las configuraciones globales y sus propios puertos TCP.
- Un Servidor de administración virtual no tiene Servidores de administración secundarios.
- Un Servidor de administración virtual no tiene otros Servidores de administración virtuales.
- En un Servidor de administración físico se ven los dispositivos, grupos, eventos y objetos de los dispositivos administrados (elementos en Cuarentena, registro de aplicaciones, etc.) de todos sus Servidores de administración virtuales.
- Un Servidor de administración virtual solo puede analizar la red con puntos de distribución conectados.

# Administración de dispositivos móviles con Kaspersky Endpoint Security para Android

Los dispositivos móviles con Kaspersky Endpoint Security para Android™ instalado (denominados, en lo sucesivo, dispositivos KES) se administran por medio del Servidor de administración. Kaspersky Security Center admite las siguientes funciones para administrar dispositivos KES:

- Manejo de dispositivos móviles como dispositivos cliente:
  - Membrecía en grupos de administración
  - Supervisión, por ejemplo, ver estados, eventos e informes
  - Modificación de la configuración local y asignación de directivas para Kaspersky Endpoint Security para Android
- Envío de comandos en modo centralizado
- Instalación de paquetes de aplicaciones móviles remotamente

El Servidor de administración administra los dispositivos KES mediante TLS, puerto TCP 13292.

# Despliegue y configuración inicial

Kaspersky Security Center es una aplicación distribuida. Kaspersky Security Center incluye las aplicaciones siguientes:

- Servidor de administración: El componente principal, diseñado para administrar los dispositivos de una organización y almacenar datos en un DBMS.
- Consola de administración: La herramienta básica para el administrador. La Consola de administración se envía junto con el Servidor de administración, pero también se puede instalar individualmente en uno o varios dispositivos ejecutados por el administrador.
- Kaspersky Security Center Web Console: Una interfaz web para el Servidor de administración diseñada para las operaciones básicas. Puede instalar este componente en cualquier dispositivo que cumpla requisitos de software y hardware.
- Agente de red: diseñado para administrar la aplicación de seguridad instalada en un dispositivo, así como para recopilar información sobre ese dispositivo. Los agentes de red se instalan en dispositivos de una organización.

El despliegue de Kaspersky Security Center en la red de una organización se realiza de la siguiente manera:

- Instalación de un Servidor de administración.
- Instalación de Kaspersky Security Center Web Console.
- Instalación de la Consola de administración en el dispositivo del administrador.
- Instalación del Agente de red y aplicación de seguridad en dispositivos de la empresa.

# Recomendaciones sobre la instalación del Servidor de administración

Esta sección contiene recomendaciones sobre cómo para instalar el Servidor de administración. Esta sección también proporciona situaciones sobre cómo usar una carpeta compartida en el dispositivo del Servidor de administración a fin de instalar el Agente de red en los dispositivos cliente.

## Creación de cuentas para los servicios del Servidor de administración en un clúster de conmutación por error

De forma predeterminada, el instalador automáticamente crea cuentas no privilegiadas para servicios del Servidor de administración. Este comportamiento es el más conveniente para la instalación del Servidor de administración en un dispositivo común.

Sin embargo, la instalación del Servidor de administración en un clúster de conmutación por error requiere una situación diferente:

1. Crear cuentas de dominio sin privilegios para los servicios del Servidor de administración convertirlas en miembros del grupo de seguridad de dominio global llamado KLAdmins.

2. En el instalador del Servidor de administración, especificar las cuentas de dominio que se han creado para los servicios.

## Selección de un DBMS

Al seleccionar el sistema de administración de bases de datos (DBMS) para utilizarlo en un Servidor de administración, debe tener en cuenta el número de dispositivos cubiertos por el Servidor de administración.

La siguiente tabla enumera las opciones de DBMS válidas, así como las recomendaciones y las restricciones en su uso.

Recomendaciones y restricciones en DBMS

| DBMS | Recomendaciones y restricciones |
|---|---|
| SQL Server Express Edition 2016 o posterior | Utilice este DBMS si planea ejecutar un solo Servidor de administración para menos de 10 000 dispositivos.<br>Se recomienda deshabilitar la Tarea del inventario del software y deshabilitar (en la configuración de directivas de Kaspersky Endpoint Security) las notificaciones del Servidor de administración en las aplicaciones iniciadas.<br>Puede limitar el número máximo de eventos en el repositorio de eventos para evitar el desbordamiento de la base de datos.<br>Consulte el siguiente tema para más detalles: Evaluación de espacio de la base de datos.<br>El uso simultáneo del DBMS de SQL Server Express Edition por el Servidor de administración y otras aplicaciones está estrictamente prohibido.<br>La base de datos de Microsoft SQL Express no es compatible con la tarea **Sincronización con Windows Update**. |
| Edición de SQL Server local, no Express, 2016 o posterior | Sin limitaciones. |

| DBMS | Recomendaciones y restricciones |
| --- | --- |
| Edición de SQL Server remota, no Express, 2016 o posterior | Solo es válido si ambos dispositivos están en el mismo dominio de Windows®; Si los dominios difieren, se debe establecer una relación de confianza bidireccional entre ellos. |
| MySQL 5.5, 5.6 o 5.7 local o remoto (ya no se admiten las versiones 5.5.1, 5.5.2, 5.5.3, 5.5.4 y 5.5.5 de MySQL) | Utilice este DBMS si planea ejecutar un solo Servidor de administración para menos de 10 000 dispositivos.<br>Se recomienda deshabilitar la Tarea del inventario del software y deshabilitar (en la configuración de directivas de Kaspersky Endpoint Security) las notificaciones del Servidor de administración en las aplicaciones iniciadas. Consulte el siguiente tema para más detalles: Evaluación de espacio de la base de datos. |
| MySQL 8.0.20 o versión posterior local o remoto | Utilice este DBMS si planea ejecutar un solo Servidor de administración para menos de 50 000 dispositivos.<br>Se recomienda deshabilitar la Tarea del inventario del software y deshabilitar (en la configuración de directivas de Kaspersky Endpoint Security) las notificaciones del Servidor de administración en las aplicaciones iniciadas. Consulte el siguiente tema para más detalles: Evaluación de espacio de la base de datos. |
| MariaDB local o remota (ver versiones compatibles) | Utilice este DBMS si planea ejecutar un solo Servidor de administración para menos de 20 000 dispositivos.<br>Se recomienda deshabilitar la Tarea del inventario del software y deshabilitar (en la configuración de directivas de Kaspersky Endpoint Security) las notificaciones del Servidor de administración en las aplicaciones iniciadas. Consulte el siguiente tema para más detalles: Evaluación de espacio de la base de datos. |
| PostgreSQL, Postgres Pro (ver versiones compatibles) | Utilice uno de estos DBMS si planea ejecutar un solo Servidor de administración para menos de 50 000 dispositivos.<br>Se recomienda deshabilitar la Tarea del inventario del software y deshabilitar (en la configuración de directivas de Kaspersky Endpoint Security) las notificaciones del Servidor de administración en las aplicaciones iniciadas. Consulte el siguiente tema para más detalles: Evaluación de espacio de la base de datos. |

Si usa un DBMS PostgreSQL, MariaDB o MySQL, la pestaña **Eventos** puede mostrar una lista incompleta de eventos para el dispositivo cliente seleccionado. Esto ocurre cuando el DBMS almacena una gran cantidad de eventos. Realice una de las siguientes acciones si desea aumentar la cantidad de eventos mostrados:

- Eliminación de eventos innecesarios.
- Reducción del plazo de almacenamiento para eventos innecesarios.

Para ver una lista completa de eventos registrados en el Servidor de administración para el dispositivo, use Informes.

Si está utilizando SQL Server 2019 como DBMS y no tiene el parche acumulativo CU12 o posterior, debe realizar lo siguiente después de instalar Kaspersky Security Center:

1. Conéctese a SQL Server con SQL Management Studio.
2. Ejecute los siguientes comandos (si elige un nombre diferente para la base de datos, use ese nombre en lugar de KAV):

```
USE KAV
GO
ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
GO
```

3. Reinicie el servicio SQL Server 2019.

De lo contrario, el uso de SQL Server 2019 puede generar errores, como "There is insufficient system memory in resource pool 'internal' to run this query" (Memoria de sistema insuficiente en el grupo de recursos interno para ejecutar esta consulta).

## Especificación de la dirección del Servidor de administración

Al instalar el Servidor de administración, debe especificar la dirección externa del Servidor de administración. Esta dirección se utilizará como dirección predeterminada al crear paquetes de instalación del Agente de red. Después de esto, podrá cambiar la dirección del equipo host del Servidor de administración usando herramientas de la Consola de administración; la dirección no cambiará automáticamente en paquetes de instalación del Agente de red que ya hayan creado.

# Configuración de protección en la red de una organización cliente

Después de que la instalación del Servidor de administración se haya completado, la Consola de administración se inicia y le solicita que realice la instalación inicial a través del Asistente relevante. Cuando el Asistente de inicio rápido se está ejecutando, las siguientes directivas y tareas se crean en el grupo de administración original:

- Directiva de Kaspersky Endpoint Security.
- Tarea de grupo para actualizar Kaspersky Endpoint Security.
- Tarea de grupo para analizar un dispositivo con Kaspersky Endpoint Security.
- Directiva del Agente de red.
- Tarea de análisis de vulnerabilidades (tarea del Agente de red).
- Tarea de instalación de actualizaciones y reparación de vulnerabilidades (tarea del Agente de red).

Las directivas y las tareas se crean con las configuraciones predeterminadas, que pueden resultar ser subóptimas o incluso inadmisibles para la organización. Por lo tanto, debe comprobar las propiedades de objetos que se han creado y modificarlos manualmente, si es necesario.

Esta sección contiene la información sobre la configuración manual de directivas, tareas y otras configuraciones del Servidor de administración e información sobre el punto de distribución, lo que crea una estructura del grupo de administración y la jerarquía de tareas, y otra configuración.

## Configuración manual de la directiva de Kaspersky Endpoint Security

Esta sección proporciona recomendaciones sobre cómo configurar la directiva de Kaspersky Endpoint Security, que es creada por el Asistente de inicio rápido. Puede establecer la configuración en la ventana de propiedades de la directiva.

Cuando modifique un ajuste, recuerde hacer clic en el ícono de bloqueo ubicado sobre el ajuste para poder usar su valor en una estación de trabajo.

## Configuración de la directiva en la sección Protección avanzada contra amenazas

Para obtener una descripción completa de los ajustes disponibles en esta sección, consulte la documentación de Kaspersky Endpoint Security para Windows.

En la sección **Protección avanzada contra amenazas**, puede configurar el uso de Kaspersky Security Network para Kaspersky Endpoint Security para Windows. También puede configurar Kaspersky Endpoint Security para Windows, como detección de comportamiento, prevención de exploits, Prevención de intrusiones en el host y motor de reparación.

En la subsección **Kaspersky Security Network**, le recomendamos que active la opción **Kaspersky Security Network**. Esta función ayuda a redistribuir y optimizar el tráfico de la red. Si la opción **Kaspersky Security Network** está deshabilitada, puede habilitar el uso directo de servidores KSN.

## Configuración de la directiva en la sección Protección básica contra amenazas

Para obtener una descripción completa de los ajustes disponibles en esta sección, consulte la documentación de Kaspersky Endpoint Security para Windows.

En la sección **Protección básica contra amenazas** de la ventana de propiedades de la directiva, le recomendamos que especifique configuraciones adicionales en las subsecciones **Firewall** y **Protección contra amenazas de archivo**.

La subsección **Firewall** contiene ajustes que le permiten controlar la actividad de red de las aplicaciones en los dispositivos cliente. Un dispositivo cliente utiliza una red a la que se le ha asignado alguno de estos estados: pública, local o de confianza. Kaspersky Endpoint Security puede permitir o bloquear el tráfico de red en un dispositivo basándose en el estado de la red. Cuando agregue una nueva red a su organización, deberá asignarle un estado de red adecuado. Si el dispositivo cliente es, por ejemplo, una computadora portátil, recomendamos que el dispositivo use una red pública o de confianza, ya que la computadora portátil no siempre está conectada a la red local. En la subsección **Firewall** puede verificar si ha asignado correctamente estados a las redes utilizadas en su organización.

*Para revisar la lista de redes:*

1. En las propiedades de la directiva, vaya a **Protección básica contra amenazas** → **Firewall**.
2. En la sección **Redes disponibles**, haga clic en el botón **Configuración**.
3. En la ventana **Firewall** que se abre, vaya a la pestaña **Redes** para ver la lista de redes.

En la subsección **Protección contra amenazas de archivo** puede desactivar el análisis de las unidades de red. El análisis de unidades de red puede tener un impacto pronunciado en las unidades. Es preferible realizar análisis indirectos en los servidores de archivos.

*Para deshabilitar el análisis de unidades de red:*

1. En las propiedades de la directiva, vaya a **Protección básica contra amenazas → Protección contra amenazas de archivo**.
2. En la sección **Nivel de seguridad**, haga clic en el botón **Configuración**.
3. En la ventana **Protección contra amenazas de archivo** que se abre, en la ficha **General**, desmarque la casilla **Todas las unidades de red**.

## Configuración de la directiva en la sección Configuración general

Para obtener la descripción completa de la configuración disponible en esta sección, consulte la documentación de Kaspersky Endpoint Security.

A continuación, se describen algunas acciones de configuración adicionales que recomendamos realizar en la ventana de propiedades de la directiva de Kaspersky Endpoint Security, en la sección **Configuración general**.

### Sección Configuración general, subsección Informes y almacenamiento

En la sección **Transferencia de datos al Servidor de administración**, encontrará la casilla **Acerca de las aplicaciones iniciadas**. Cuando esta casilla está seleccionada, la base de datos del Servidor de administración guarda la información acerca de todas las versiones de todos los módulos de software en los dispositivos en red. Esta información puede requerir una cantidad significativa de espacio en disco en la base de datos de Kaspersky Security Center (docenas de gigabytes). Por lo tanto, si la casilla **Acerca de las aplicaciones iniciadas** aún está seleccionada en la directiva de alto nivel, se debe desmarcar.

### Sección Configuración general, subsección Interfaz

Si la protección de amenazas en la red de la organización se debe administrar en el modo centralizado a través de la Consola de administración, debe deshabilitar la visualización de la interfaz de usuario de Kaspersky Endpoint Security en las estaciones de trabajo (desactive la casilla **Mostrar interfaz de la aplicación** en la sección **Interacción con el usuario**) y habilitar la protección con contraseña (marque la casilla **Habilitar protección con contraseña** en la sección **Protección con contraseña**).

## Configuración de la directiva en la sección Configuración de eventos

En la sección **Configuración de eventos**, debe deshabilitar el almacenamiento de cualquier evento en el Servidor de administración, excepto los siguientes:

- En la pestaña **Crítico**:
  - *La autoejecución de la aplicación está deshabilitada*
  - *Acceso denegado*
  - *Inicio de aplicación prohibido*
  - *No se puede desinfectar*
  - *Contrato de licencia de usuario final infringido*
  - *No se pudo cargar el módulo de cifrado*
  - *No se pueden iniciar dos tareas al mismo tiempo*
  - *Se detectó una amenaza activa; ejecute la Desinfección avanzada*
  - *Ataque de red detectado*
  - *No se actualizaron todos los componentes*
  - *Error de activación*
  - *Error al habilitar el modo portátil*
  - *Error de interacción con Kaspersky Security Center*
  - *Error al deshabilitar el modo portátil*
  - *Error al cambiar los componentes de la aplicación*
  - *Error al implementar las reglas de cifrado o descifrado de archivos*
  - *No se puede aplicar la directiva*
  - *Proceso finalizado*
  - *Actividad de red bloqueada*
- En la pestaña **Error funcional**: *La configuración de la tarea no es válida y no se aplicó*

- En la pestaña **Advertencia**:
  - *Autoprotección deshabilitada*
  - *Clave de reserva incorrecta*
  - *El usuario optó por no implementar la directiva de cifrado*
- En la ficha **Información**: *Inicio de aplicación prohibido en el modo de prueba*

## Configuración manual de la tarea de grupo para actualizar Kaspersky Endpoint Security

Si el Servidor de administración actúa como origen de actualización, la opción de programación óptima y recomendada para Kaspersky Endpoint Security es **Cuando se descargan nuevas actualizaciones en el repositorio** con la casilla **Usar retardo aleatorio automático para el inicio de tareas** marcada.

Si se crea una tarea local para descargar actualizaciones de servidores de Kaspersky al repositorio en cada punto de distribución, la programación periódica será óptima y recomendada para la tarea de actualización del grupo de Kaspersky Endpoint Security. En este caso, el valor del intervalo de aleatorización debería configurarse en 1 hora.

## Instalación manual de la tarea de grupo para analizar un dispositivo con Kaspersky Endpoint Security

El Asistente de inicio rápido crea una tarea de grupo para analizar un dispositivo. De forma predeterminada, la tarea tiene asignada la programación **Ejecutar los viernes a las 7:00 p. m.** con aleatorización automática y la casilla de verificación **Ejecutar tareas no realizadas** no está marcada.

Esto significa que si los dispositivos de la organización se apagan, por ejemplo, los viernes a las 6:30 p. m., la tarea de análisis de los dispositivos nunca se ejecutará. Debe configurar la programación más cómoda para esta tarea según las reglas del lugar de trabajo adoptadas en la organización.

## Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas

El Asistente de inicio rápido crea la tarea *Buscar vulnerabilidades y actualizaciones requeridas* para el Agente de red. De forma predeterminada, se asigna a la tarea la programación **Ejecutar los martes a las 7:00 p. m.** con aleatorización automática, y la casilla **Ejecutar tareas no realizadas** está marcada.

Si las reglas del lugar de trabajo de la organización especifican el cierre de todos los dispositivos a esta hora, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* se ejecutará después de que los dispositivos se vuelvan a encender; es decir, el miércoles por la mañana. Esto puede ser inconveniente porque los análisis de vulnerabilidades pueden hacer que aumente la carga en los subsistemas de disco y CPU. Debe buscar que la programación de la tarea se adecue a las reglas dispuestas por su organización.

# Configuración manual de la tarea de grupo para la instalación de actualizaciones y la reparación de vulnerabilidades

El Asistente de inicio rápido crea una tarea de grupo para la instalación de actualizaciones y la reparación de vulnerabilidades para el Agente de red. De forma predeterminada, la tarea está configurada para ejecutarse todos los días a la 1:00 a. m. con una demora definida al azar automáticamente, y la opción **Ejecutar tareas no realizadas** no debe estar habilitada.

Si las reglas del lugar de trabajo de la organización especifican el cierre de dispositivos durante la noche, la instalación de actualizaciones nunca se ejecutará. Debe configurar la programación más cómoda para esta tarea de análisis de vulnerabilidades según las reglas del lugar de trabajo adoptadas en la organización. También es importante tener en cuenta que la instalación de actualizaciones puede requerir reiniciar el dispositivo.

# Creación de una estructura de grupos de administración y asignación de puntos de distribución

Una estructura de grupos de administración en Kaspersky Security Center realiza las funciones siguientes:

- Configura el alcance de las directivas.

  Existe otra forma de aplicar ajustes pertinentes en dispositivos: mediante el uso de perfiles de directiva. En este caso, el alcance de las directivas está configurado, por ejemplo, con etiquetas, ubicaciones del dispositivo en unidades organizacionales de Active Directory y membrecía en grupos de seguridad de Active Directory.

- Configura el alcance de las tareas de grupo.

  Existe un modo de definir el alcance de las tareas de grupo que no depende de una jerarquía de grupos de administración: el uso de tareas para selecciones de dispositivos y de tareas para dispositivos específicos.

- Regula la capacidad de acceder a los distintos dispositivos, Servidores de administración secundarios y Servidores de administración virtuales.

- Asigna puntos de distribución.

Al momento de crear la estructura de grupos de administración, para que la asignación de puntos de distribución sea óptima, es necesario tener en cuenta la topología de la red de la organización. La distribución óptima de puntos de distribución le permite ahorrar tráfico en la red de la organización.

Según el organigrama de la empresa y la topología de red adoptada por el cliente MSP, pueden aplicarse las siguientes configuraciones estándares a la estructura de grupos de administración:

- Oficina única

- Varias pequeñas oficinas separadas

## Configuración estándar de un cliente MSP: oficina única

En una configuración estándar de "oficina única", todos los dispositivos se encuentran en la red de la organización y tienen la capacidad de "verse" los unos a los otros. La red de la organización puede constar de varias partes independientes (redes o segmentos de red) vinculadas por canales estrechos.

Los siguientes métodos pueden emplearse para armar la estructura de grupos de administración:

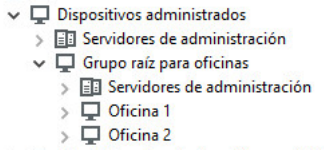
- Armar la estructura de grupos de administración tomando en cuenta la topología de la red. No es necesario que la estructura de grupos de administración refleje con absoluta precisión la topología de la red. Es suficiente con que haya coincidencia entre las partes independientes de la red y ciertos grupos de administración. Puede usar la asignación automática de puntos de distribución o asignarlos manualmente.

- Armar la estructura de grupos de administración sin tener en cuenta la topología de la red. En este caso, debe deshabilitar la asignación automática de puntos de distribución y luego asignar uno o varios dispositivos para que actúen como puntos de distribución para un grupo de administración original en cada una de las partes independientes de la red; por ejemplo, para el grupo **Dispositivos administrados**. Todos los puntos de distribución estarán al mismo nivel y presentarán el mismo alcance en todos los dispositivos en la red de la organización. En este caso, cada Agente de red se conectará al punto de distribución que tenga la ruta más corta. La ruta a un punto de distribución se puede determinar con la utilidad tracert.

## Configuración estándar de un cliente MSP: varias pequeñas oficinas remotas

Esta configuración estándar permite contar con varias pequeñas oficinas remotas, que pueden o no comunicarse con la oficina de la sede central mediante Internet. Cada oficina remota está ubicada detrás de una pasarela NAT; debido a ello, las oficinas remotas están aisladas las unas de las otras y no se pueden conectar entre sí.

La configuración se debe ver reflejada en la estructura de grupos de administración: debe crearse un grupo de administración independiente para cada oficina remota (los grupos **Oficina 1** y **Oficina 2** en la siguiente imagen).




Oficinas remotas incluidas en la estructura de grupos de administración

Se debe asignar uno o varios puntos de distribución a cada grupo de administración que corresponda a una oficina. Los puntos de distribución deben ser dispositivos que se encuentren en la oficina remota y deben tener una cantidad suficiente de espacio libre en disco. Los dispositivos incluidos en el grupo **Oficina 1** accederán a los puntos de distribución asignados al grupo de administración **Oficina 1**, por ejemplo.

Cuando hay usuarios que utilizan una computadora portátil para trabajar físicamente en más de una oficina, resulta necesario designar, junto con los puntos de distribución existentes, dos o más dispositivos en cada oficina remota para que actúen como puntos de distribución de un grupo de administración ubicado en un nivel superior (el grupo llamado **Grupo para oficinas** en la imagen anterior).

Ejemplo: Una computadora portátil incluida en el grupo de administración **Oficina 1** se traslada físicamente a la oficina que corresponde al grupo de administración **Oficina 2**. Luego del traslado, el Agente de red de la computadora portátil intenta acceder a los puntos de distribución asignados al grupo **Oficina 1**, pero esos puntos de distribución no están disponibles. Tras ello, el Agente de red intenta acceder a los puntos de distribución asignados al **Grupo para oficinas**. Como las oficinas remotas están aisladas entre sí, los intentos de acceder a los puntos de distribución asignados al grupo de administración **Grupo para oficinas** solo tendrán éxito cuando el Agente de red intente acceder a los puntos de distribución del grupo **Oficina 2**. Así, la computadora portátil permanecerá en el grupo de administración correspondiente a su oficina inicial, pero usará el punto de distribución de la oficina en la que se encuentre físicamente.

# Jerarquía de directivas, usando perfiles de directivas

En esta sección se proporciona información sobre cómo aplicar directivas a los dispositivos en los grupos de administración. Esta sección también proporciona información sobre los perfiles de directivas.

## Jerarquía de directivas

En Kaspersky Security Center, usa directivas para definir una sola colección de configuración para múltiples dispositivos. Por ejemplo, el alcance de la directiva de la aplicación P definido para el grupo de administración G incluye los dispositivos administrados que tienen la aplicación P instalada y que se han agregado al grupo G o a cualquiera de sus subgrupos, excepto los subgrupos donde la casilla **Heredar del grupo primario** está desmarcada en las propiedades.

Una directiva se diferencia de cualquier parámetro local por los candados (🔒) que aparecen al lado de su configuración. Si una configuración (o un grupo de configuraciones) está bloqueada en las propiedades de la directiva, debe usar, en primer lugar, esta configuración (o grupo de configuraciones) al crear la configuración vigente y, en segundo lugar, debe escribir la configuración o el grupo de configuraciones en la directiva descendente.

La creación de la configuración vigente en un dispositivo se puede describir de la forma siguiente: los valores de toda la configuración que no se hayan bloqueado se toman desde la directiva, a continuación se sobrescriben con los valores de la configuración local, y luego la recolección resultante se sobrescribe con los valores de la configuración bloqueada tomada desde la directiva.

Las directivas de la misma aplicación se afectan mutuamente a través de la jerarquía de grupos de administración: la configuración bloqueada desde la directiva descendente sobrescribe la misma configuración desde la directiva descendente.

Hay una directiva especial para los usuarios fuera de la oficina. Esta directiva entra en vigor en un dispositivo cuando el dispositivo cambia al modo fuera de la oficina. Las directivas fuera de la oficina no afectan a otras directivas a través de la jerarquía de grupos de administración.

## Perfiles de directivas

En muchas circunstancias, puede ser inconveniente aplicar directivas a dispositivos solo mediante la jerarquía de grupos de administración. Puede ser necesario crear varias instancias de una sola directiva que se diferencien en una o dos configuraciones para grupos de administración diferentes, y sincronizar los contenidos de esas directivas en el futuro.

Para ayudarle a evitar tales problemas, Kaspersky Security Center admite *perfiles de directivas*. Un perfil de directiva es un subconjunto nominado de los valores de configuración definidos en una directiva. Este subconjunto se distribuye en dispositivos de destino junto con la directiva, y se complementa bajo una condición específica denominada *Condición de activación del perfil*. Los perfiles solo contienen configuraciones que se diferencian de la directiva "básica" que está activa en el dispositivo cliente (equipo o dispositivo móvil). Al activarse un perfil se modifica la configuración de directiva que se encontraba activa en el dispositivo antes de que se activara el perfil. Dicha configuración tomará los valores que se habían especificado en el perfil.

Las restricciones siguientes se imponen actualmente en los perfiles de directivas:

- Una directiva puede incluir un máximo de 100 perfiles.
- Un perfil de directivas no puede contener otros perfiles.
- Un perfil de directivas no puede contener una configuración de notificaciones.

## Contenido de un perfil

Un perfil de directivas contiene las siguientes partes:

- Perfiles de nombre con nombres idénticos que se afectan mutuamente a través de la jerarquía de grupos de administración con reglas comunes.
- Subconjunto de configuración de la directiva. A diferencia de la directiva, que contiene todas las configuraciones, un perfil solo contiene configuraciones que realmente se requieren (configuraciones bloqueadas).
- La condición de activación es una expresión lógica con propiedades del dispositivo. Un perfil está activo (complementa a la directiva) solo cuando la condiciones de activación del perfil se hace verdadera. En todos los otros casos, el perfil está inactivo y es ignorado. Las propiedades del dispositivo siguientes se pueden incluir en esa expresión lógica:
  - Estado de modo fuera de la oficina.
  - Propiedades del entorno de la red; nombre de la regla activa para conexión con el Agente de red.
  - Presencia o ausencia de etiquetas específicas en el dispositivo.
  - El hecho de que el dispositivo pertenezca a una unidad de Active Directory, sea esta relación de pertenencia explícita (el dispositivo se encuentra en la unidad organizativa especificada) o implícita (el dispositivo está en una unidad organizativa que se encuentra dentro de la unidad especificada, sin importar el nivel de anidamiento).
  - Membrecía del dispositivo en un grupo de seguridad de Active Directory (explícita o implícita).
  - Membrecía del propietario del dispositivo en un grupo de seguridad de Active Directory (explícita o implícita).
- Casilla de deshabilitación del Perfil. Los perfiles deshabilitados siempre se ignoran y sus condiciones de activación respectivas no se verifican.
- Prioridad del Perfil. Las condiciones de activación de perfiles diferentes son independientes, por lo tanto varios perfiles se pueden activar simultáneamente. Si los perfiles activos contienen recolecciones no superpuestas de configuraciones, no se producirá ningún problema. Sin embargo, si dos perfiles activos contienen valores diferentes de la misma configuración, una ambigüedad ocurrirá. Esta ambigüedad se debe evitar a través de prioridades del perfil: El valor de la variable ambigua se tomará desde el perfil que tiene la prioridad más alta (el que se califica más alto en la lista de perfiles).

### Comportamiento de los perfiles cuando las directivas se afectan mutuamente a través de la jerarquía

Los perfiles con el mismo nombre se fusionan según las reglas de fusión de directivas. Los perfiles de una directiva ascendente tienen una prioridad más alta que los perfiles de una directiva descendente. Si la edición de la configuración se prohíbe en la directiva ascendente (está bloqueada), la directiva descendente usa las condiciones de activación del perfil de la ascendente. Si la edición de la configuración está permitida en la directiva ascendente, las condiciones de activación del perfil desde la directiva descendente se utilizan.

Como un perfil de directivas puede contener la propiedad **El dispositivo no tiene conexión** en su condición de activación, los perfiles reemplazan completamente la función de las directivas para los usuarios fuera de la oficina, que ya no se admitirán.

Una directiva para usuarios fuera de la oficina puede contener perfiles, pero sus perfiles solo se pueden activar después de que el dispositivo cambie al modo fuera de la oficina.

## Tareas

Kaspersky Security Center administra las aplicaciones de seguridad de Kaspersky instaladas en los dispositivos mediante la creación y ejecución de *tareas*. Las tareas son el medio que se utiliza para instalar, iniciar y detener aplicaciones, analizar archivos, actualizar bases de datos y módulos de software y realizar otras acciones en las aplicaciones.

Las tareas para una aplicación específica solo se pueden crear si el complemento de administración para esa aplicación está instalado.

Una tarea se puede ejecutar en el Servidor de administración o en un dispositivo.

Las siguientes tareas se realizan en el Servidor de administración:

- Distribución automática de informes
- Descarga de actualizaciones en el repositorio del Servidor de administración
- Copia de seguridad de los datos del Servidor de administración
- Mantenimiento de la base de datos
- Sincronización con Windows Update
- Creación de un paquete de instalación basado en la imagen del SO de un dispositivo de referencia

Los siguientes tipos de tareas se ejecutan en los dispositivos:

- *Tareas locales*. Son tareas que se ejecutan en un dispositivo específico.

  Las tareas locales pueden ser modificadas por el administrador usando herramientas de la Consola de administración, o por el usuario de un dispositivo remoto (por ejemplo, a través de la interfaz de aplicaciones de seguridad). Si el administrador y el usuario del dispositivo administrado modifican una tarea local al mismo tiempo, los cambios realizados por el administrador se consideran prioritarios y son los que entran en vigor.

- *Tareas de grupo*. Son tareas que se ejecutan en todos los dispositivos de un grupo específico.

  A menos que se especifique lo contrario en las propiedades de la tarea, una tarea de grupo también afecta a todos los subgrupos del grupo seleccionado. Una tarea de grupo también afecta (opcionalmente) a los dispositivos que se han conectado a Servidores de administración secundarios y virtuales incluidos en el grupo o en cualquiera de sus subgrupos.

- Tareas globales. Son tareas que se ejecutan en un conjunto de dispositivos que pueden o no pertenecer a un grupo.

Para cada aplicación, puede crear cualquier número de tareas de grupo, tareas globales o tareas locales.

Puede copiar, importar, exportar y eliminar tareas, consultar el progreso de su ejecución y modificar su configuración.

Para que una tarea se inicie en un dispositivo, la aplicación para la que se la ha creado debe estar en ejecución.

Los resultados de las tareas se guardan en el registro de eventos de Microsoft Windows y en el registro de eventos de Kaspersky Security Center, tanto de forma centralizada en el Servidor de administración como localmente en cada dispositivo.

No incluya datos privados en la configuración de las tareas. Por ejemplo, evite especificar la contraseña del administrador del dominio.

## Reglas de movimiento de dispositivos

Recomendamos que automatice la asignación de dispositivos a grupos de administración en el servidor virtual que corresponda a un cliente MSP con *reglas de movimiento de dispositivos*. Una regla de movimiento de dispositivos consiste en tres partes principales: nombre, condición de ejecución (expresión lógica con atributos del dispositivo) y grupo de administración de destino. Una regla mueve un dispositivo al grupo de administración de destino si los atributos del dispositivo cumplen la condición de ejecución de la regla.

Toda regla de movimiento de dispositivos tiene una prioridad. El Servidor de administración comprueba los atributos del dispositivo en cuanto a si cumplen con la condición de ejecución de cada regla, en orden ascendente de prioridad. Si los atributos del dispositivo cumplen con la condición de ejecución de una regla, el dispositivo se mueve al grupo de destino, y con esto cesa el procesamiento de la regla en este dispositivo. Si los atributos de dispositivo cumplen con las condiciones de varias reglas, el dispositivo se mueve al grupo de destino de la regla con la prioridad más alta (es decir, la que tiene la clasificación más alta en la lista de reglas).

Las reglas de movimiento de dispositivos se pueden crear implícitamente. Por ejemplo, en las propiedades de un paquete de instalación o una tarea de instalación remota, puede especificar el grupo de administración al cual el dispositivo se debe mover después de que Agente de red se instala en este. Además, las reglas de movimiento de dispositivos pueden ser creadas explícitamente por el administrador de Kaspersky Security Center, en la lista de reglas de movimiento. La lista se localiza en la Consola de administración, en las propiedades del grupo de **Dispositivos no asignados**.

La regla de movimiento predeterminada está diseñada para la asignación inicial de dispositivos a grupos de administración, que se ejecuta una sola vez. La regla mueve dispositivos desde el grupo de **Dispositivos no asignados** solo una vez. Si un dispositivo se movió una vez mediante esta regla, la regla no lo volverá a mover, incluso si devuelve el dispositivo al grupo de **Dispositivos no asignados** manualmente. Este es el modo recomendado de aplicar las reglas de movimiento.

Puede mover dispositivos que ya se han asignado a algunos grupos de administración. Para hacer esto, en las propiedades de una regla, desactive la casilla **Solo mover dispositivos que no pertenezcan a un grupo de administración**.

Aplicar reglas de movimiento a dispositivos que ya se han asignado a algunos grupos de administración aumenta considerablemente la carga en el Servidor de administración.

Puede crear una regla móvil que afectaría a un dispositivo solo repetidamente.

Recomendamos encarecidamente no mueva un solo dispositivo desde un grupo al otro repetidamente (por ejemplo, a fin de aplicar una directiva especial a ese dispositivo, ejecutar una tarea de grupo especial o actualizar el dispositivo a través de un punto de distribución específico).

Tales situaciones no se admiten, porque aumentan la carga en el Servidor de administración y el tráfico de red a un grado extremo. Estas situaciones también entran en conflicto con los principios operativos de Kaspersky Security Center (en particular en el área de derechos de acceso, eventos e informes). Se debe encontrar otra solución; por ejemplo, a través del uso de perfiles de directivas, tareas para selecciones de dispositivos, asignación de Agentes de red según el escenario estándar, entre otras cosas.

## Categorización del software

La herramienta principal para supervisar la ejecución de aplicaciones son las *categorías de Kaspersky* (en adelante también conocidas como *categorías KL*). Las categorías de KL ayudan a los administradores de Kaspersky Security Center a simplificar la asistencia de la clasificación del software y minimizan el tráfico hacia los dispositivos administrados.

Las categorías de usuario solo se deben crear para aplicaciones que no se pueden clasificar en ninguna de las categorías KL existentes (por ejemplo, para el software personalizado). Las categorías de usuario se crean sobre la base de un paquete de instalación de la aplicación (MSI) o una carpeta con paquetes de instalación.

Si está disponible una colección grande de software que no se ha clasificado a través de categorías KL, puede ser útil crear una categoría actualizada automáticamente. Las sumas de control de archivos ejecutables automáticamente se agregarán a esta categoría en cada modificación de la carpeta que contiene paquetes de distribución.

No cree categorías de software actualizadas automáticamente para las carpetas Mis documentos, %windir%, %ProgramFiles% y %ProgramFiles(x86)%. El conjunto de archivos en estas carpetas está sujeto a cambios frecuentes, lo que lleva a una carga aumentada en el Servidor de administración y tráfico de red aumentado. Debe crear una carpeta dedicada con la colección de software y periódicamente agregar elementos nuevos elementos a ella.

## Acerca de las aplicaciones multiinquilino

Kaspersky Security Center permite que los administradores de los proveedores de servicios y los administradores de los inquilinos utilicen las aplicaciones de Kaspersky compatibles con el multiinquilinato. Una vez que una aplicación multiinquilino de Kaspersky se instala en la infraestructura del proveedor de servicios, los inquilinos pueden comenzar a usarla.

Para separar las tareas y directivas relacionadas con los distintos inquilinos, se debe crear un Servidor de administración virtual dedicado a cada inquilino en Kaspersky Security Center. Las tareas y directivas de las aplicaciones multiinquilino deben crearse para el grupo de administración Dispositivos administrados del Servidor de administración virtual correspondiente al inquilino que utiliza esas aplicaciones. Los dispositivos de los inquilinos no se verán afectados por las tareas que se creen para los grupos de administración vinculados al Servidor de administración principal.

A diferencia de los administradores de un proveedor de servicios, el administrador de un inquilino solamente puede ver y crear tareas y directivas para los dispositivos del inquilino con el que está asociado. Los grupos de tareas y los parámetros de directivas a los que tienen acceso estas dos clases de administradores no son los mismos. Los administradores de los inquilinos no pueden acceder a ciertas tareas y parámetros de directivas.

En el contexto de la estructura jerárquica de un inquilino, las directivas que se crean para las aplicaciones multiinquilino se heredan tanto en los grupos de administración de nivel inferior como en los de nivel superior; las directivas se propagan a todos los dispositivos cliente que pertenecen al inquilino.

# Copia de seguridad y restauración de la configuración del Servidor de administración

La copia de seguridad de la configuración del Servidor de administración y su base de datos se realiza a través de la tarea de copia de seguridad y la utilidad klbackup. Una copia de seguridad incluye toda la configuración principal y objetos que pertenecen al Servidor de administración, por ejemplo, certificados, claves maestras para el cifrado de unidades en dispositivos administrados, claves para varias licencias, estructura de grupos de administración con todos sus contenidos, tareas, directivas, etc. Con una copia de seguridad puede recuperar la operación de un Servidor de administración cuanto antes, lo que puede demorar de una docena de minutos a un par de horas.

Si ninguna copia de seguridad está disponible, un error puede llevar a una pérdida irrevocable de certificados y toda la configuración del Servidor de administración. Esto requerirá a configurar de nuevo Kaspersky Security Center desde el principio y realizar la distribución inicial del Agente de red en la red de la organización de nuevo. Todas las claves principales para el cifrado de unidades en dispositivos administrados también se perderán, arriesgando la pérdida irrevocable de datos cifrados en dispositivos con Kaspersky Endpoint Security. Por ese motivo, no debe descuidar las copias de seguridad habituales del Servidor de administración usando la tarea de copia de seguridad estándar.

El Asistente de inicio rápido crea la tarea de copia de seguridad para la configuración del Servidor de administración y lo configura para que se ejecute a diario, a las 4:00 a. m. Las copias de seguridad se guardan de forma predeterminada en la carpeta %ALLUSERSPROFILE%\Application Data\KasperskySC.

Si una instancia de Microsoft SQL Server instalada en otro dispositivo se utiliza como DBMS, debe modificar la tarea de copia de seguridad al especificar una ruta de UNC, que está disponible para escritura tanto de parte del servicio del Servidor de administración como del servicio de SQL Server, como la carpeta para almacenar copias de seguridad. Este requisito se deriva de una característica especial de copia de seguridad en DBMS de Microsoft SQL Server.

Si una instancia local de Microsoft SQL Server se utiliza como DBMS, también recomendamos guardar copias de seguridad en un medio dedicado a fin de asegurarlos contra el daño junto con el Servidor de administración.

Como una copia de seguridad contiene datos importantes, la tarea de copia de seguridad y la utilidad klbackup aseguran la protección con contraseña de copias de seguridad. De forma predeterminada, la tarea de copia de seguridad se crea con una contraseña en blanco. Debe configurar una contraseña en las propiedades de la tarea de copia de seguridad. Descuidar este requisito causa una situación donde todas las claves de certificados del Servidor de administración, las claves para licencias y las claves principales para el cifrado de unidades en dispositivos administrados permanecen no cifradas.

Además de la copia de seguridad habitual, también debe crear una copia de seguridad antes de cada cambio significativo, incluida la instalación de actualizaciones del Servidor de administración y los parches.

Si utiliza Microsoft SQL Server como DBMS, puede minimizar el tamaño de las copias de seguridad. Para ello, habilite la opción **Comprimir copia de seguridad** en la configuración de SQL Server.

Para restaurar una copia de seguridad, deberá utilizar la utilidad klbackup en una instancia del Servidor de administración que se acabe de instalar, que esté en funcionamiento y que sea de la misma versión para la que se haya creado la copia de seguridad (o de una versión más reciente).

La instancia del Servidor de administración en el cual se debe realizar la restauración debe utilizar un DBMS del mismo tipo (por ejemplo, el mismo SQL Server o MariaDB) y la misma versión o una posterior. La versión del Servidor de administración puede ser igual (con un parche idéntico o posterior) o posterior.

Esta sección describe situaciones estándares para restaurar la configuración y objetos del Servidor de administración.

## Un dispositivo con el Servidor de administración es inoperable

Si un dispositivo con el Servidor de administración es inoperable debido a un error, se recomiendan realizar las siguientes acciones:

- Se debe asignar al nuevo Servidor de administración la misma dirección: nombre NetBIOS, FQDN o IP estática (dependiendo de cuál se haya definido al instalarse los Agentes de red).
- Instalar el Servidor de administración usando un DBMS del mismo tipo, de la misma versión (o una posterior). Puede instalar la misma versión del Servidor con el mismo parche (o uno posterior), o una versión posterior. Después de la instalación, no realice la instalación inicial a través del Asistente.
- En el menú **Iniciar**, ejecute la utilidad klbackup y realice la restauración.

## La configuración del Servidor de administración o la base de datos es corrupta

Si el Servidor de administración es inoperable debido a configuración o la base de datos corruptas (por ejemplo, después de una sobrecarga eléctrica), se recomienda usar la siguiente situación de restauración:

1. Analice el sistema de archivos en el dispositivo dañado.
2. Desinstale la versión inoperable del Servidor de administración.
3. Reinstale el Servidor de administración usando un DBMS del mismo tipo y de la misma versión (o una posterior). Puede instalar la misma versión del Servidor con el mismo parche (o uno posterior), o una versión posterior. Después de la instalación, no realice la instalación inicial a través del Asistente.
4. En el menú **Iniciar**, ejecute la utilidad klbackup y realice la restauración.

Se prohíbe restaurar el Servidor de administración de cualquier modo diferente de a través de la utilidad klbackup.

Cualquier intento de restaurar el Servidor de administración a través de un software de terceros llevará inevitablemente a la desincronización de datos en los nodos de Kaspersky Security Center de la aplicación distribuida y, por consiguiente, al funcionamiento inadecuado de la aplicación.

# Despliegue del Agente de red y de la aplicación de seguridad

Para administrar dispositivos en una organización, tiene que instalar el Agente de red en cada uno de ellos. La distribución de Kaspersky Security Center distribuido en dispositivos corporativos normalmente comienza con la instalación del Agente de red en ellos.

En Microsoft Windows XP, el Agente de red podría no realizar las siguientes operaciones correctamente: descargar actualizaciones directamente desde los servidores de Kaspersky (como un punto de distribución); funcionar como servidor proxy de KSN (como un punto de distribución); detectar vulnerabilidades de terceros (si se usa la Administración de vulnerabilidades y parches).

## Despliegue inicial

Si el Agente de red se ha instalado en un dispositivo, la instalación remota de aplicaciones en ese dispositivo se realiza a través de este Agente de red. El paquete de distribución de una aplicación que se debe instalar se transfiere a través de canales de comunicación entre Agentes de red y el Servidor de administración, junto con la configuración de instalación definida por el administrador. Para transferir el paquete de distribución, puede usar nodos de distribución de relevo, es decir puntos de distribución, distribución multidifusión, etc. Para obtener más información sobre cómo instalar aplicaciones en dispositivos administrados con el Agente de red ya instalado, consulte la siguiente información en esta sección.

Puede realizar la instalación inicial del Agente de red en dispositivos que ejecuten Windows usando uno de los métodos siguientes:

- Con herramientas de terceros para la instalación remota de aplicaciones.
- Con directivas de grupo de Windows: usando herramientas de administración de Windows estándares para directivas de grupo.
- En el modo forzado, usando opciones especiales en la tarea de instalación remota de Kaspersky Security Center.
- Al enviar vínculos de usuarios del dispositivo a paquetes independientes generados por Kaspersky Security Center. Los paquetes independientes son módulos ejecutables que contienen los paquetes de distribución de aplicaciones seleccionadas con su configuración definida.
- Manualmente, mediante la ejecución de instaladores de la aplicación en los dispositivos.

En plataformas que no sean de Microsoft Windows, debe realizar la instalación inicial del Agente de red en los dispositivos administrados mediante las herramientas de terceros existentes, o manualmente, mediante el envío a los usuarios un archivo con un paquete de distribución configurado previamente. Puede actualizar el Agente de red a una versión nueva o instalar otras aplicaciones de Kaspersky en plataformas diferentes de Windows, usando Agentes de red (ya instalados en dispositivos) para realizar tareas de instalación remotas. En este caso, la instalación es idéntica a la que se realiza en equipos que ejecutan Microsoft Windows.

Al seleccionar un método y una estrategia para instalar las aplicaciones en una red administrada, debe considerar varios factores (lista parcial):

- Configuración de la red corporativa.
- Número total de dispositivos.
- La presencia de dominios de Windows en la red administrada, la posibilidad de modificar directivas de grupo de Active Directory en esos dominios.
- El reconocimiento de las cuentas de usuario con derechos de administrador locales en los dispositivos en los que se planeó el despliegue inicial de las aplicaciones de Kaspersky (es decir, la disponibilidad de una cuenta de usuario de dominio con derechos de administrador locales o la presencia de cuentas de usuario locales unificadas con derechos de administrador en esos dispositivos).
- El tipo de conexión y el ancho de banda de los canales de red entre el Servidor de administración y las redes del cliente MSP, así como el ancho de banda de los canales dentro de esas redes.
- Configuración de la seguridad aplicada en dispositivos remotos al inicio del despliegue (por ejemplo, el uso de UAC y modo simple de uso compartido de archivos).

## Configuración de instaladores

Antes de desplegar las aplicaciones de Kaspersky en una red, debe especificar la configuración de instalación, es decir, los parámetros que se configuran durante la instalación de la aplicación. Al instalar el Agente de red, debe especificar, como mínimo, una dirección para la conexión con el Servidor de administración y la configuración del proxy; también se pueden requerir algunos parámetros avanzados. Según el método de instalación que haya seleccionado, puede definir la configuración de varias formas. En el caso más sencillo (instalación interactiva manual en un dispositivo seleccionado), toda la configuración relevante puede definirse mediante la interfaz de usuario del instalador, por lo que, en algunos casos, la instalación inicial incluso puede realizarse mediante el envío a usuarios de un enlace al paquete de distribución del Agente de red junto con la configuración (dirección del Servidor de administración, etc.) que el usuario debe ingresar en la Interfaz del instalador.

No se recomienda usar este método, ya que puede causar problemas a los usuarios, dado que implica un alto riesgo de errores al definir la configuración manualmente; además, no puede utilizarse con la instalación no interactiva de aplicaciones en grupos del dispositivo. En general, el administrador debe especificar valores para la configuración en el modo centralizado; esos valores se pueden utilizar posteriormente para la creación de paquetes independientes. Los paquetes independientes son archivos de extracción automática que contienen paquetes de distribución con la configuración definida por el administrador. Los paquetes independientes pueden ubicarse en recursos que permiten tanto la descarga por parte de usuarios finales (por ejemplo, en Servidor web de Kaspersky Security Center) como la instalación no interactiva en dispositivos en red seleccionados.

## Paquetes de instalación

El primer método y el principal de definición de la configuración de instalación de aplicaciones es de uso múltiple y, por consiguiente, conveniente para todos los métodos de instalación, tanto con herramientas de Kaspersky Security Center como con la mayor parte de herramientas de terceros. Este método consiste en crear paquetes de instalación de aplicaciones en Kaspersky Security Center.

Los paquetes de instalación se generan usando los métodos siguientes:

- Automáticamente, desde paquetes de distribución especificados, sobre la base de *descriptores* incluidos (archivos con la extensión kud que contienen reglas para instalación y análisis de resultados y otra información).

- Desde archivos ejecutables de instaladores o instaladores en formato Microsoft Windows Installer (MSI), para aplicaciones estándar o compatibles.

Los paquetes de instalación generados se organizan jerárquicamente como carpetas, con subcarpetas y archivos. Además del paquete de distribución original, un paquete de instalación contiene la configuración editable (incluida la configuración del instalador y reglas para procesar tales casos como la necesidad de reiniciar el sistema operativo a fin de completar la instalación), así como los módulos auxiliares menores.

Los valores de configuración de la instalación que son específicos para que se admita una aplicación seleccionada pueden especificarse en la interfaz de usuario de la Consola de administración al crear un paquete de instalación (encontrará más configuración en las propiedades de un paquete de instalación que ya se ha creado). Al realizar la instalación remota de aplicaciones mediante herramientas de Kaspersky Security Center, se entregan paquetes de instalación a dispositivos de destino de modo que la ejecución del instalador de una aplicación ponga toda la configuración definida por los administradores a disposición. Al usar herramientas de terceros para la instalación de aplicaciones de Kaspersky, solo debe garantizar la disponibilidad del paquete de instalación completo en el dispositivo de destino, es decir, la disponibilidad del paquete de distribución y su configuración. Kaspersky Security Center crea y almacena los paquetes de instalación en una subcarpeta dedicada de la carpeta de datos compartida.

No especifique ningún detalle de cuentas privilegiadas en los parámetros de los paquetes de instalación.

Para obtener instrucciones sobre el uso de este método de configuración para las aplicaciones de Kaspersky antes de instalarlas a través de herramientas de terceros, consulte la sección "Despliegue mediante directivas de grupo de Microsoft Windows".

Inmediatamente después de la instalación de Kaspersky Security Center, unos paquetes de instalación se generan automáticamente; están listos para la instalación e incluyen paquetes del Agente de red y paquetes de aplicaciones de seguridad para Microsoft Windows.

En algunos casos, la utilización de paquetes de instalación para instalar aplicaciones en una red del cliente MSP implica la necesidad de crear paquetes de instalación en Servidores virtuales que correspondan a clientes MSP. La creación de paquetes de instalación en Servidores virtuales le permite usar diferente configuración de instalación para diferentes clientes MSP. En la primera instancia, esto resulta útil al gestionar paquetes de instalación del Agente de red, ya que los Agentes de red instalados en las redes de los diferentes clientes MSP utilizan diferentes direcciones para conectarse al Servidor de administración. En realidad, la dirección de conexión determina el Servidor al cual se conecta el Agente de red.

Además de la posibilidad de crear nuevos paquetes de instalación inmediatamente en un Servidor de administración virtual, el modo de operación principal para los paquetes de instalación en Servidores de administración virtuales es la "distribución" de paquetes de instalación del Servidor de administración principal a Servidores de administración virtuales. Puede distribuir paquetes de instalación seleccionados (o todos) a Servidores de administración virtuales seleccionados (incluidos todos los Servidores dentro de un grupo de administración seleccionado) con la tarea del Servidor de administración correspondiente. Además, puede seleccionar la lista de paquetes de instalación del Servidor de administración principal al crear un nuevo Servidor de administración virtual. Los paquetes que ha seleccionado se distribuirán inmediatamente al Servidor de administración virtual recién creado.

Al distribuir un paquete de instalación, su contenido no se copia completamente. El repositorio del archivo en un Servidor de administración virtual, que corresponde al paquete de instalación que se distribuido, solo almacena archivos de la configuración específica de ese Servidor virtual. La parte principal del paquete de instalación (incluido el paquete de distribución de la aplicación que se instala) permanece sin alterar; solo se almacena en el repositorio del Servidor de administración principal. Esto le permite aumentar el rendimiento del sistema drásticamente y reducir el volumen de disco requerido. Al gestionar paquetes de instalación distribuidos a Servidores de administración virtuales (es decir, al ejecutar tareas de instalación remotas o crear paquetes de instalación independientes), los datos del paquete de instalación original del Servidor de administración principal "se fusionan" con los archivos de configuración, que corresponden al paquete distribuido en el Servidor de administración virtual.

Aunque la clave de licencia para una aplicación puede configurarse en las propiedades del paquete de instalación, es aconsejable evitar este método de distribución de la licencia, ya que es sencillo obtener accidentalmente acceso de lectura a los archivos en la carpeta. Lo que hay que hacer es usar claves de licencia de distribución automática o tareas de instalación de claves de licencia.

## Propiedades MSI y archivos de transformación

Otro modo de configurar la instalación en la plataforma de Windows es definir propiedades MSI y archivos de transformación. Este método puede utilizarse al realizar la instalación mediante herramientas de terceros destinadas para instaladores en el formato de Microsoft Installer, así como al realizar la instalación mediante directivas de grupo de Windows usando herramientas de Microsoft estándares u otras herramientas de terceros diseñadas para gestionar directivas de grupo de Windows.

## Despliegue con herramientas de terceros para la instalación remota de aplicaciones

Si en la organización se cuenta con herramientas para la instalación remota de aplicaciones (por ejemplo Microsoft System Center), es conveniente realizar el despliegue inicial con esas herramientas.

Se deben ejecutar las siguientes acciones:

- Seleccionar el método para configurar la instalación que se adapte mejor a la herramienta de despliegue que se utilizará.
- Definir el mecanismo de sincronización entre la modificación de la configuración de paquetes de instalación (a través de la interfaz de la Consola de administración) y la operación de determinadas herramientas de terceros usadas para el despliegue de aplicaciones a partir de los datos del paquete de instalación.

## Información general sobre las tareas de instalación remotas en Kaspersky Security Center

Kaspersky Security Center proporciona una amplia variedad de métodos para la instalación remota de aplicaciones, que se implementan como tareas de instalación remotas. Puede crear una tarea de instalación remota tanto para un grupo de administración especificado como para dispositivos específicos o una selección de dispositivos (tales tareas se muestran en la Consola de administración, en la carpeta **Tareas**). Al crear una tarea, puede seleccionar paquetes de instalación (los del Agente de red u otra aplicación) que se instalarán dentro de esta tarea, así como especificar ciertas configuraciones que definan el método de la instalación remota.

Las Tareas para grupos de administración afectan a ambos dispositivos incluidos en un grupo especificado y todos los dispositivos en todos los subgrupos dentro de ese grupo de administración. Una tarea cubre dispositivos de Servidores de administración secundarios incluidos en un grupo o cualquiera de sus subgrupos si la configuración correspondiente se habilita en la tarea.

Las tareas para dispositivos específicos actualizan la lista de dispositivos cliente en cada ejecución de acuerdo con el contenido de la selección en el momento en el que se inicia la tarea. Si una selección incluye dispositivos que se han conectado a Servidores de administración secundarios, la tarea también se ejecutará en esos dispositivos.

Para asegurar la operación correcta de una tarea de instalación remota en dispositivos conectados a Servidores de administración secundarios, debe usar la tarea de distribución para distribuir paquetes de instalación usados por su tarea a los Servidores de administración secundarios correspondientes de antemano.

## Despliegue mediante directivas de grupo de Microsoft Windows

Se recomienda que realice el despliegue inicial del Agente de red a través de directivas de grupo de Microsoft Windows si las condiciones siguientes se cumplen:

- El dispositivo es miembro de un dominio de Active Directory.
- El acceso al controlador de dominio se concede con los derechos de administrador, que le permiten crear y modificar directivas de grupo de Active Directory.
- Los paquetes de instalación configurados pueden moverse a la red que aloja los dispositivos administrados (a una carpeta compartida que está disponible para su lectura para todos los dispositivos de destino).
- El esquema de despliegue permite esperar al siguiente reinicio de rutina de los dispositivos de destino antes de comenzar a instalar el Agente de red en ellos (o puede forzar la aplicación de una directiva de grupo de Windows en esos dispositivos).

Este esquema de despliegue consiste en lo siguiente:

- El paquete de distribución de aplicaciones en el formato de Microsoft Installer (paquete MSI) se localiza en una carpeta compartida (una carpeta donde las cuentas de LocalSystem de dispositivos de destino tienen permisos de lectura).
- En la directiva de grupo de Active Directory, un objeto de instalación se crea para el paquete de distribución.

- El alcance de instalación está configurado al especificar la unidad organizativa (OU) o el grupo de seguridad, que incluye los dispositivos de destino.

- La próxima vez que un dispositivo de destino inicia sesión en el dominio (antes de que los usuarios del dispositivo inicien sesión en el sistema), todas las aplicaciones instaladas se examinan para ver la presencia de la aplicación requerida. Si la aplicación no se encuentra, el paquete de distribución se descarga desde el recurso especificado en la directiva y se instala a continuación.

Una ventaja de este esquema de despliegue consiste en que las aplicaciones asignadas se instalan en los dispositivos de destino mientras el sistema operativo se está cargando, es decir, incluso antes de que el usuario inicie sesión en el sistema. Aun si un usuario con derechos suficientes elimina la aplicación, se instalará de nuevo en el siguiente inicio del sistema operativo. El defecto de este esquema de despliegue es que los cambios hechos por el administrador a la directiva de grupo no entrarán en vigor hasta que los dispositivos se reinicien (si no se usa ninguna herramienta adicional).

Puede usar directivas de grupo para instalar tanto el Agente de red como otras aplicaciones si sus instaladores respectivos están en el formato de Windows Installer.

La instalación del Agente de red desde el paquete MSI solo es posible en modo silencioso, no se admite la instalación interactiva desde el paquete MSI.

Asimismo, cuando selecciona este método de despliegue, también debe evaluar la carga en el recurso de archivo del cual se copiarán los archivos a los dispositivos de destino después de aplicar la directiva de grupo de Windows. También debe elegir el método de entrega del paquete de instalación configurado a ese recurso, así como el método de sincronización de los cambios relevantes en su configuración.

## Manipulación de directivas de Microsoft Windows a través de la tarea de instalación remota de Kaspersky Security Center

Este método de despliegue solo está disponible si es posible acceder al controlador de dominio, que contiene los dispositivos de destino, desde el dispositivo del Servidor de administración, mientras que la carpeta compartida del Servidor de administración (el que almacena los paquetes de instalación) es accesible para su lectura desde dispositivos de destino. Debido a los motivos indicados anteriormente, este método de despliegue no se considera aplicable al MSP.

## Instalación no asistida de aplicaciones a través de directivas de Microsoft Windows

El administrador puede crear objetos requeridos para la instalación en una directiva de grupo de Windows en su propio nombre. En este caso, debe cargar los paquetes a un servidor de archivos independiente y proporcionar un enlace a ellos.

Las situaciones de instalación siguientes son posibles:

- El administrador crea un paquete de instalación y configura sus propiedades en la Consola de administración. A continuación, el administrador copia la subcarpeta EXEC completa de este paquete desde la carpeta compartida de Kaspersky Security Center a una carpeta en un recurso del archivo dedicado de la organización. El objeto de la directiva de grupo proporciona un enlace al archivo MSI de este paquete almacenado en la subcarpeta del recurso del archivo dedicado de la organización.

- El administrador descarga el paquete de distribución de aplicaciones (incluyendo el del Agente de red) de Internet y lo carga en el recurso del archivo dedicado de la organización. El objeto de la directiva de grupo proporciona un enlace al archivo MSI de este paquete almacenado en la subcarpeta del recurso del archivo dedicado de la organización. La configuración de instalación se define al configurar las propiedades MSI o al configurar los archivos de transformación MST.

## Despliegue forzado con la tarea de instalación remota de Kaspersky Security Center

Para desplegar por primera vez el Agente de red u otras aplicaciones, puede forzar la instalación de los paquetes de instalación seleccionados con la tarea de instalación remota de Kaspersky Security Center, siempre que cada dispositivo tenga una cuenta de usuario con derechos de administrador local.

La instalación forzada también se puede usar si no se puede acceder directamente a los dispositivos mediante el Servidor de administración: por ejemplo, los dispositivos están en redes aisladas o están en una red local mientras que el elemento del Servidor de administración está en la DMZ.

En el primer despliegue, el Agente de red no está instalado. Por lo tanto, en la configuración de la tarea de instalación remota, no se puede seleccionar la distribución de los archivos necesarios para la instalación de la aplicación mediante el Agente de red. Solo puede optar por distribuir archivos con recursos del sistema operativo a través del Servidor de administración o puntos de distribución.

El servicio del Servidor de administración debe ejecutarse bajo una cuenta que tenga privilegios administrativos en los dispositivos de destino. También puede especificar una cuenta que tenga acceso al recurso compartido admin$ en la configuración de la tarea de instalación remota.

> De manera predeterminada, la tarea de instalación remota se conecta a los dispositivos utilizando las credenciales de la cuenta con la cual se ejecuta el Servidor de administración; es decir, la cuenta que tiene acceso al recurso compartido admin$. Debe especificar esta cuenta en la configuración de la tarea de instalación remota solo si el Agente de red no está instalado en los dispositivos de destino.
> Al crear la tarea de instalación remota para que se ejecute en dispositivos con Linux, siempre debe especificar una cuenta para crear una conexión SSH.

Puede especificar dispositivos de destino explícitamente (con una lista), mediante la selección del grupo de administración de Kaspersky Security Center al cual pertenecen o tras crear una selección de dispositivos en función de un criterio específico. La hora de inicio de instalación es definida por la programación de la tarea. Si la configuración **Ejecutar tareas no realizadas** se habilita en las propiedades de la tarea, la tarea se puede ejecutar inmediatamente después de que los dispositivos de destino se activen, o cuando se muevan al grupo de administración de destino.

La instalación forzada consiste en el envío de paquetes de instalación a dispositivos de destino, la copia subsecuente de archivos al recurso admin$ en cada uno de los dispositivos de destino y el registro remoto de los servicios de compatibilidad en esos dispositivos. La entrega de paquetes de instalación a dispositivos de destino se realiza mediante una función de Kaspersky Security Center que garantiza la interacción de la red. Las condiciones siguientes se deben cumplir en este caso:

- Se puede acceder a los dispositivos de destino desde el Servidor de administración o desde el punto de distribución.
- La resolución del nombre para los dispositivos de destino funciona correctamente en la red.
- Los usos compartidos administrativos (admin$) permanecen activados en los dispositivos de destino.
- Los siguientes servicios del sistema están en ejecución en los dispositivos de destino:
  - Servidor (LanmanServer)

    De manera predeterminada, este servicio está en ejecución.
  - Iniciador de procesos de servidor DCOM (DcomLaunch)
  - Asignador de endpoints RPC (RpcEptMapper)
  - Llamada a procedimiento remoto (RpcSs)
- El puerto TCP 445 está abierto en los dispositivos de destino para permitir el acceso remoto a través de herramientas de Windows.

  TCP 139, UDP 137 y UDP 138 se usan en protocolos más antiguos y ya no son necesarios para las aplicaciones actuales.

  En el firewall, se deben permitir puertos de acceso saliente dinámicos para las conexiones desde el Servidor de administración y los puntos de distribución a los dispositivos de destino.
- Se permiten configuraciones de seguridad de la política de dominio de Active Directory para el funcionamiento del protocolo NTLM durante el despliegue del Agente de red.
- En los dispositivos de destino que ejecutan Microsoft Windows XP, el modo de uso compartido simple de archivos está deshabilitado.
- En los dispositivos de destino, el modelo de seguridad y uso compartido de acceso se configura como *Clásico: los usuarios locales se autentican como ellos mismos*. De ninguna manera puede ser *Invitado únicamente: los usuarios locales se autentican como invitados*.
- Los dispositivos de destino son miembros del dominio, o bien se crean cuentas uniformes con derechos de administrador en los dispositivos de destino de antemano.

Para desplegar correctamente el Agente de red u otras aplicaciones en un dispositivo que no está unido a un dominio de Active Directory de Windows Server 2003 o posterior, debe deshabilitar el Control de cuentas de usuario (UAC) remoto en el dispositivo. UAC remoto es una de las razones que impide que las cuentas de administradores locales accedan a admin$, lo que es necesario para el despliegue forzado del Agente de red u otras aplicaciones. Si deshabilita UAC remoto, no interfiere con UAC local.

Durante la instalación en dispositivos nuevos que todavía no se han asignado a ninguno de los grupos de administración de Kaspersky Security Center, puede abrir las propiedades de la tarea de instalación remota y especificar el grupo de administración al cual los dispositivos se moverán después de la instalación del Agente de red.

Al crear una tarea de grupo, tenga en cuenta que cada tarea de grupo afecta a todos los dispositivos en todos los grupos anidados dentro de un grupo seleccionado. Por lo tanto, debe evitar duplicar las tareas de instalación en los subgrupos.

Una forma simplificada de crear tareas para la instalación forzada de aplicaciones es la instalación automática. Para hacerlo, abra las propiedades del grupo de administración, abra la lista de paquetes de instalación y seleccione los que se deben instalar en dispositivos de este grupo. Como resultado, los paquetes de instalación seleccionados se instalarán automáticamente en todos los dispositivos de este grupo y todos sus subgrupos. El intervalo de tiempo durante el cual los paquetes se instalarán depende del rendimiento de la red y el número total de dispositivos conectados a una red.

Para reducir la carga en el Servidor de administración durante la entrega de paquetes de instalación a dispositivos de destino, puede seleccionar la instalación a través de puntos de distribución en la tarea de instalación. Tenga en cuenta que este método de instalación aplica una carga significativa a dispositivos que actúan como puntos de distribución. Por lo tanto, se recomienda seleccionar dispositivos que cumplan con los requisitos de los puntos de distribución. Si usa puntos de distribución, debe asegurarse de que estén presentes en cada una de las subredes aisladas que alojan los dispositivos de destino.

El uso de puntos de distribución como centros de instalación locales también puede ser útil al realizar la instalación en dispositivos en subredes comunicadas con el Servidor de administración mediante un canal de capacidad reducida, mientras que un canal más amplio está disponible entre dispositivos en la misma subred.

El espacio libre del disco en la partición con la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit debe superar, en gran cantidad, el tamaño total de los paquetes de distribución de aplicaciones instaladas.

## Ejecución de paquetes independientes creados por Kaspersky Security Center

Los métodos anteriormente descritos para el despliegue inicial del Agente de red y de otras aplicaciones no siempre se pueden implementar porque no es posible cumplir con todas las condiciones aplicables. En tales casos, puede crear un archivo ejecutable común llamado un *paquete de instalación independiente* a través de Kaspersky Security Center, usando paquetes de instalación con la configuración de instalación relevante preparada por el administrador. Un paquete de instalación independiente puede publicarse en un Servidor web interno (incluido en Kaspersky Security Center) si esto se considera razonable (se configuró el acceso externo a ese Servidor web para usuarios de dispositivos de destino), o en un Servidor web que viene incluido en Kaspersky Security Center Web Console. También puede copiar paquetes independientes a otro Servidor web.

Puede usar Kaspersky Security Center para enviar a usuarios seleccionados un mensaje de correo electrónico que contenga un vínculo al archivo del paquete independiente en el Servidor web que se utilice actualmente, solicitándoles ejecutar el archivo (ya sea en modo interactivo o con la clave "-s" para la instalación silenciosa). Puede adjuntar el paquete de instalación independiente a un mensaje de correo electrónico y luego enviarlo a los usuarios de dispositivos que no tengan acceso al Servidor web. El administrador también puede copiar el paquete independiente a un dispositivo externo, entregarlo a un dispositivo relevante, y luego ejecutarlo más adelante.

Puede crear un paquete independiente desde un paquete del Agente de red, un paquete de otra aplicación (por ejemplo, la aplicación de seguridad), o ambos. Si el paquete independiente se ha creado desde el Agente de red y otra aplicación, la instalación se inicia con el Agente de red.

Al crear un paquete independiente con el Agente de red, puede especificar el grupo de administración en el cual los dispositivos nuevos (esos que no se han asignado a ninguno de los grupos de administración) automáticamente se moverá cuando la instalación del Agente de red se complete en ellos.

Los paquetes independientes se pueden ejecutar en el modo interactivo (de forma predeterminada), mostrando el resultado para la instalación de aplicaciones que contienen, o se pueden ejecutar en el modo silencioso (cuando se ejecutan con la clave "-s"). El modo silencioso se puede utilizar para la instalación desde scripts (por ejemplo, desde scripts configurados para ejecutarse tras la instalación de una imagen de sistema operativo). El resultado de instalación en el modo silencioso está determinado por el código de devolución del proceso.

### Opciones para la instalación manual de aplicaciones

Los administradores o los usuarios experimentados pueden instalar las aplicaciones manualmente en el modo interactivo. Pueden usar los paquetes de distribución originales o paquetes de instalación generados por ellos y almacenados en la carpeta compartida de Kaspersky Security Center. De forma predeterminada, los instaladores se ejecutan en modo interactivo y les indican a los usuarios todos los valores requeridos. Sin embargo, al ejecutar el proceso setup.exe desde el origen de un paquete de instalación con la clave "-s", el instalador se ejecutará en el modo silencioso y con la configuración que se ha definido al configurar el paquete de instalación.

> Al ejecutarse setup.exe desde el origen de un paquete de instalación, el paquete se copiará primero a una carpeta local temporal, y luego el instalador de la aplicación se ejecutará desde la carpeta local.

## Instalación remota de aplicaciones en dispositivos en los que se encuentra instalado el Agente de red

Si un Agente de red operable conectado al Servidor de administración principal (o a alguno de sus Servidores secundarios) está conectado en un dispositivo, puede actualizar el Agente de red en este dispositivo, así como instalar, actualizar o eliminar cualquier aplicación admitida a través del Agente de red.

Puede habilitar esta opción al seleccionar la casilla **Con el Agente de red** en las propiedades de la tarea de instalación remota.

Si esta casilla se selecciona, los paquetes de instalación con la configuración de instalación definida por el administrador se transferirán a los dispositivos de destino a través de canales de comunicación entre l Agente de red y el Servidor de administración.

Para optimizar la carga del Servidor de administración y minimizar el tráfico entre el Servidor de administración y los dispositivos, es útil asignar puntos de distribución en cada red remota o en cada dominio de transmisión (consulte las secciones Acerca de los puntos de distribución y Creación de una estructura de grupos de administración y asignación de puntos de distribución). En este caso, los paquetes de instalación y la configuración del instalador se distribuyen desde el Servidor de administración hacia los dispositivos de destino a través de puntos de distribución.

Además, puede usar puntos de distribución para la transmisión (multidifusión) y la distribución de paquetes de instalación, lo que permite reducir el tráfico de red considerablemente a la hora de instalar aplicaciones en forma remota.

Al transferir paquetes de instalación a los dispositivos de destino a través de canales de comunicación entre los Agentes de red y el Servidor de administración, todos los paquetes de instalación que se han preparado para la transferencia también se almacenarán en cache en la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. Al usar múltiples paquetes de instalación de gran tamaño y de diversos tipos e involucrar a un gran número de puntos de distribución, el tamaño de esta carpeta puede aumentar significativamente.

Los archivos no se pueden eliminar desde la carpeta FTServer manualmente. Cuando los paquetes de instalación originales se eliminen, los datos correspondientes automáticamente se eliminarán de la carpeta FTServer.

Todos los datos recibidos en el lado de los puntos de distribución se guardan a la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp.

Los archivos no se pueden eliminar de la carpeta $FTCITmp manualmente. Como las tareas usan los datos de esta carpeta completa, los contenidos de esta carpeta se eliminarán automáticamente.

Como los paquetes de instalación se distribuyen por canales de comunicación entre el Servidor de administración y los Agentes de red desde un repositorio intermedio en un formato optimizado para transferencias de red, ningún cambio se permite en paquetes de instalación almacenados en la carpeta original de cada paquete de instalación. Esos cambios no serán automáticamente registrados por el Servidor de administración. Si tiene que modificar los archivos de los paquetes de instalación manualmente (aunque se recomiendan evitar esta situación), debe modificar cualquiera de las configuraciones de un paquete de instalación en la Consola de administración. La modificación de la configuración de un paquete de instalación en la Consola de administración hace que el Servidor de administración actualice la imagen del paquete en el caché que se ha preparado para la transferencia hacia los dispositivos de destino.

## Opciones para controlar el reinicio de los dispositivos en la tarea de instalación remota

Los dispositivos a menudo necesitan un reinicio para completar la instalación remota de aplicaciones (en particular en Windows).

Si usa la tarea de instalación remota de Kaspersky Security Center, en el Asistente para crear nueva tarea o en la ventana de propiedades de la tarea que se ha creado (sección **Reinicio del sistema operativo**), puede seleccionar la acción para realizar cuando el dispositivo de Windows requiera un reinicio:

- **No reiniciar el dispositivo**. En este caso, ningún reinicio automático se realizará. Para completar la instalación, debe reiniciar el dispositivo (por ejemplo, manualmente o a través de la tarea de administración del dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para tareas de instalación en servidores y otros dispositivos donde la operación continua sea crítica.

- **Reiniciar el dispositivo**. En este caso, el dispositivo siempre se reinicia automáticamente si se requiere un reinicio para la finalización de la instalación. Esta opción es útil para tareas de instalación en dispositivos que proporcionan pausas habituales en su operación (cierre o reinicio).

- **Solicitar al usuario una acción**. En este caso, el recordatorio de reinicio se muestra en la pantalla del dispositivo cliente, que le solicita al usuario que lo reinicie manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). La opción **Solicitar al usuario una acción** es la más conveniente para las estaciones de trabajo donde los usuarios necesitan la posibilidad de seleccionar el horario más cómodo para un reinicio.

## Conveniencia de actualizar las bases de datos en el paquete de instalación de una aplicación antivirus

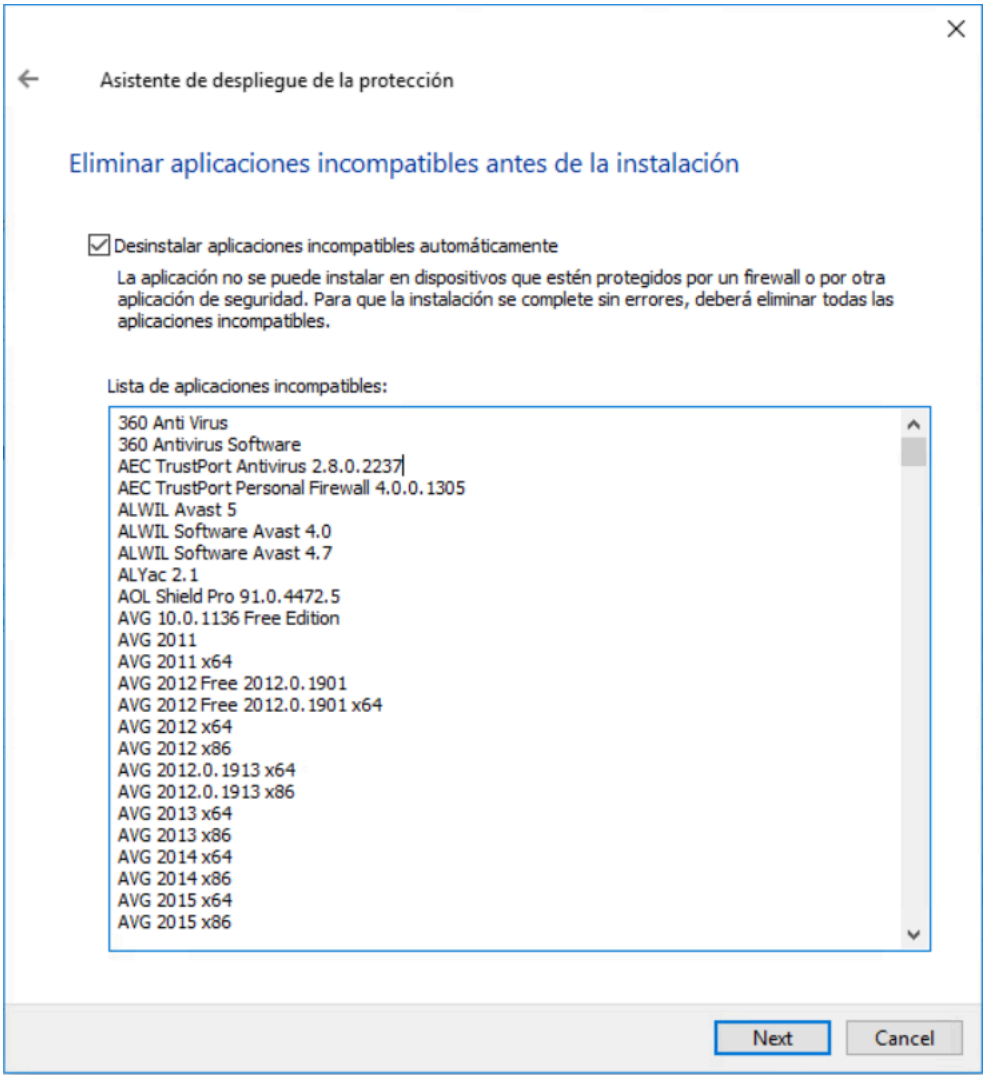
Antes de comenzar con el despliegue de la protección, debe tener en cuenta la posibilidad de actualizar las bases de datos antivirus (incluidos los módulos de los parches automáticos), que se envían junto con el paquete de distribución de la aplicación de seguridad. Es útil actualizar las bases de datos en el paquete de instalación de la aplicación antes de dar inicio al despliegue (por ejemplo, usando el comando correspondiente en el menú contextual de un paquete de instalación seleccionado). Con ello se reducirá el número de reinicios necesarios para completar el despliegue de la protección en los dispositivos de destino. Si su instalación remota involucra paquetes de instalación que se han transmitido a Servidores virtuales desde el Servidor de administración principal, solo debe actualizar las bases de datos en el paquete original en el Servidor principal. En este caso, no es necesario que actualice bases de datos en paquetes transmitidos en Servidores virtuales.

## Eliminación de las aplicaciones de seguridad de terceros incompatibles

La Instalación de aplicaciones de seguridad de Kaspersky a través de Kaspersky Security Center puede requerir la eliminación del software de terceros incompatible con la aplicación instalada. Hay dos modos principales de eliminar las aplicaciones de terceros.

## Eliminación automática de aplicaciones incompatibles usando el instalador

Cuando ejecuta el instalador, muestra una lista de aplicaciones que no son compatibles con una aplicación de Kaspersky:




La lista de aplicaciones incompatibles se muestra en el Asistente de instalación remota

Kaspersky Security Center detecta software incompatible. De forma acorde, puede seleccionar la casilla de verificación **Desinstalar aplicaciones incompatibles automáticamente** para continuar la instalación. Si desmarca la selección de esta casilla de verificación y no desinstala el software incompatible, se producirá el error y no se instalará la aplicación de Kaspersky.

Varios tipos de instalaciones admiten la eliminación automática de aplicaciones incompatibles.

## Eliminar aplicaciones incompatibles a través de una tarea dedicada

Para eliminar aplicaciones incompatibles, use la tarea *Desinstalar aplicación de forma remota*. Esta tarea se debe ejecutar en los dispositivos antes que la tarea para instalar la aplicación de seguridad. Por ejemplo, en la tarea de instalación, puede seleccionar **Al completarse otra tarea** como tipo de programación, en el que la otra tarea es *Desinstalar aplicación de forma remota*.

Este método de desinstalación es útil cuando el instalador de la aplicación de seguridad no puede eliminar correctamente una aplicación incompatible.

# Eliminar el Agente de red protegido con contraseña desde el símbolo del sistema

Para desinstalar de forma remota el Agente de red para el que estableció una contraseña de desinstalación, puede usar el símbolo del sistema.

Si pierde u olvida la contraseña del Agente de red protegido con contraseña, que está instalado en el dispositivo y que Kaspersky Security Center ya no administra, no podrá eliminar el Agente de red mediante la utilidad klmover, la herramienta Cleaner (cleaner.exe) o el símbolo del sistema. En este caso, deberá reinstalar el sistema operativo en el dispositivo que tiene instalado el Agente de red protegido con contraseña.

*Pasos para desinstalar el Agente de red desde el símbolo del sistema:*

1. Convierta la contraseña de desinstalación a un código hexadecimal.

   Utilice un recurso de Internet, un entorno de programación, un editor de texto u otra herramienta adecuada para convertir la contraseña en código hexadecimal.

   > Asegúrese de que el delimitador de salida utilizado para separar en partes el código hexadecimal generado esté establecido en `00`. Por ejemplo, el código hexadecimal `51 77 65 72 74 79` es incorrecto, mientras que el código hexadecimal `5100770065007200740079 00` es correcto.

2. Ingrese el siguiente comando en el símbolo del sistema y presione la tecla **ENTRAR**:

   ```
   msiexec.exe /x{<product code>} /qn KLUNINSTPASSWD=<hex code of your uninstallation password>
   ```

   Busque el código de producto del Agente de red en la siguiente tabla.

Códigos de producto del Agente de red

| Localización | Código de producto |
|---|---|
| Árabe | {FA7BF140-F356-404A-BDA3-3EF0878D7C63} |
| Búlgaro | {4DBF6741-FA51-4C14-AFD2-B7D9246995F6} |
| Checo | {478A6A0B-D177-4402-B703-808C05C56B13} |
| Inglés | {BCF4CF24-88AB-45E1-A6E6-40C8278A70C5} |
| Francés | {2924BEDA-E0D7-4DAF-A224-50D2E0B12F5B} |
| Alemán | {2F383CB3-6D7C-449D-9874-164E49E1E0F5} |
| Húngaro | {8899A4D4-D678-49F8-AD96-0B784F58D355} |
| Italiano | {DC3A3164-36B3-4FB4-B7BF-16A41C35A728} |
| Japonés | {790C176F-7780-4C84-8B9C-455F5C0E61C5} |
| Coreano | {70812A40-973B-4DA1-96B9-C2011280CD99} |
| Polaco | {1A7B331A-ABBE-4230-995E-BCD99C5A18CF} |
| Portugués | {0F05E4E5-5A89-482C-9A62-47CC58643788} |
| Rumano | {FF802D76-E241-41D3-AAB4-DC7FBD659446} |
| Ruso | {ED1C2D7E-5C7A-48D8-A697-57D1C080ABA7} |
| Chino simplificado | {FBD7C01E-49CB-4182-8714-9DB1EAE255CB} |
| Español | {F03982CF-1C5C-4E12-9F9E-D36C35E62402} |
| Español (México) | {29748B5F-D88A-4933-B614-1CCCD6EFB0B7} |
| Chino tradicional | {F6AD731A-36B4-4739-B1D4-70D6EDA35147} |
| Turco | {2475A66D-698B-4050-93FF-9B48EE82E2BA} |

## Utilización de herramientas para la instalación remota de aplicaciones en Kaspersky Security Center para ejecutar archivos ejecutables relevantes en dispositivos administrados

Mediante el Asistente de nuevo paquete, puede seleccionar cualquier archivo ejecutable y definir la configuración de la línea de comandos para ello. Para esto, puede agregar al paquete de instalación el archivo seleccionado o la carpeta completa en la cual este archivo se almacena. A continuación, debe crear la tarea de instalación remota y seleccionar el paquete de instalación que se ha creado.

Mientras la tarea se está ejecutando, el archivo ejecutable especificado con la configuración definida del comando solicitado se ejecutará en dispositivos de destino.

Si usa instaladores en el formato de Microsoft Windows Installer (MSI), Kaspersky Security Center analiza los resultados de instalación por medio de herramientas estándares.

Si una licencia de Administración de vulnerabilidades y parches está disponible, Kaspersky Security Center (al crear un paquete de instalación para cualquier aplicación admitida en el entorno corporativo) también usa reglas para la instalación y el análisis de resultados de instalación que están en su base de datos actualizable.

De otra forma, la tarea predeterminada para archivos ejecutables espera la finalización del proceso en ejecución, y de todos sus procesos secundarios. Después de la finalización de todos los procesos en ejecución, la tarea se completará correctamente sin tener en cuenta el código de devolución del proceso inicial. Para cambiar el comportamiento de esta tarea, antes de crear la tarea, tiene que modificar manualmente los archivos .kpd que fueron generados por Kaspersky Security Center en la carpeta del paquete de instalación recién creado y sus subcarpetas.

Los archivos .kpd utilizan la codificación ASCII. Los archivos .kud utilizan la codificación Unicode.

Para que la tarea no espere la finalización del proceso en ejecución, configure el valor de la configuración Wait en 0 en la sección [SetupProcessResult]:

```
[SetupProcessResult]
Wait=0
```

Para que la tarea espere solo la finalización del proceso en ejecución en Windows, no la finalización de todos los procesos secundarios, configure el valor de la configuración WaitJob en 0 en la sección [SetupProcessResult], por ejemplo:

```
[SetupProcessResult]
WaitJob=0
```

Para que la tarea se complete con éxito o devuelva un error según el código de retorno del proceso en ejecución, cree un archivo .bat ejecutable que guarde el código de error en un archivo, por ejemplo:

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

Y luego modifique los archivos .kud que generó Kaspersky Security Center en la carpeta del paquete de instalación recién creado:

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0=La instalación finalizó correctamente
[SetupMainResult_ErrorCodes]
1=Installation script error
2=Custom error
```

En este caso, cualquier código diferente de los enumerados causará la devolución de un error.

Para mostrar una cadena con un comentario sobre la finalización correcta de la tarea o un error en los resultados de la tarea, escriba breves descripciones de errores correspondientes a códigos de devolución del proceso en las secciones [SetupProcessResult_SuccessCodes] y [SetupProcessResult_ErrorCodes], por ejemplo:

```
[SetupProcessResult_SuccessCodes]
0= La instalación finalizó correctamente
3010=Se debe reiniciar el dispositivo para completar la instalación
[SetupProcessResult_ErrorCodes]
1602=instalación cancelada por el usuario
1603=Error importante durante la instalación
```

Para usar las herramientas de Kaspersky Security Center para administrar el reinicio del dispositivo (si se requiere un reinicio para completar una operación), enumere los códigos de devolución del proceso que indican que un reinicio se debe realizar, en la sección [SetupProcessResult_NeedReboot]:

```
[SetupProcessResult_NeedReboot]
3010=
```

## Supervisión del despliegue

Para supervisar el despliegue de Kaspersky Security Center y asegurarse de que una aplicación de seguridad y el Agente de red se instalen en los dispositivos administrados, tiene que comprobar el semáforo en la sección **Despliegue**. Este semáforo se localiza en el espacio de trabajo del nodo del Servidor de administración en la ventana principal de la Consola de administración. El semáforo refleja el estado del despliegue. El número de dispositivos con el Agente de red y aplicaciones de seguridad instalados se muestra al lado del semáforo. Cuando cualquier tarea de instalación se está ejecutando, puede supervisar su progreso aquí. Si se presentan errores de instalación, el número de errores se muestra aquí. Puede ver los detalles de cualquier error haciendo clic en el enlace.

También puede usar el gráfico de despliegue en el espacio de trabajo de la carpeta **Dispositivos administrados** en la pestaña **Grupos**. El gráfico refleja el proceso de despliegue, ya que muestra el número de dispositivos sin Agente de red, con Agente de red, o con Agente de red y una aplicación de seguridad.

Para obtener más información sobre el progreso del despliegue (o la operación de una tarea de instalación específica), abra la ventana de resultados de la tarea de instalación remota relevante: Haga clic en la tarea con el botón derecho del ratón y seleccione **Resultados** el menú contextual. La ventana muestra dos listas: la superior contiene los estados de las tareas en dispositivos, mientras que la inferior contiene eventos de tareas en el dispositivo que está seleccionado actualmente en la lista superior.

La información sobre los errores de despliegue se agrega al registro de eventos de Kaspersky en el Servidor de administración. La información sobre errores también está disponible en la selección correspondiente de eventos en la carpeta **Informes y notificaciones**, la subcarpeta **Eventos**.

## Configuración de instaladores

Esta sección proporciona la información sobre los archivos de instaladores de Kaspersky Security Center y la configuración de instalación, así como recomendaciones sobre cómo instalar el Servidor de administración y el Agente de red en el modo silencioso.

## Información general

Los Instaladores de los componentes de Kaspersky Security Center 15.1 (Servidor de administración, Agente de red y Consola de administración) se basan en la tecnología de Windows Installer. Un paquete MSI es el núcleo de un instalador. Este formato de paquetes permite usar todas las ventajas proporcionadas por Windows Installer: escalabilidad, disponibilidad de un sistema de parches, sistema de transformación, instalación centralizada a través de soluciones de terceros y registro transparente con el sistema operativo.

## Instalación en modo silencioso (con un archivo de respuesta)

Los instaladores de Servidor de administración y el Agente de red tienen la función de trabajar con el archivo de respuesta (ss_install.xml), donde los parámetros para la instalación en el modo silencioso sin la participación del usuario se integran. El archivo ss_install.xml se localiza en la misma carpeta que el paquete MSI; se utiliza automáticamente durante la instalación en el modo silencioso. Puede habilitar el modo de instalación silenciosa con el modificador de línea de comandos "/s".

Una descripción general de un ejemplo de ejecución se presenta a continuación:

```
setup.exe /s
```

> Antes de iniciar el instalador en modo silencioso, lea el Contrato de licencia de usuario final (también denominado EULA, por las siglas del término en inglés). Si el kit de distribución de Kaspersky Security Center no incluye un archivo TXT con el texto del EULA, puede descargar el archivo desde el sitio web de Kaspersky.

El archivo ss_install.xml es una instancia del formato interno de los parámetros del instalador de Kaspersky Security Center. Los paquetes de distribución contienen el archivo ss_install.xml con los parámetros predeterminados.

> No modifique el archivo ss_install.xml manualmente. Este archivo puede modificarse mediante las herramientas de Kaspersky Security Center al modificar los parámetros de los paquetes de instalación en la Consola de administración.

*Para modificar el archivo de respuesta para la instalación del Servidor de administración:*

1. Abra el paquete de distribución de Kaspersky Security Center. Si utiliza un archivo EXE de paquete completo, descomprímalo.
2. Desde la carpeta Server, abra la línea de comandos y ejecute el siguiente comando:
   ```
   setup.exe /r ss_install.xml
   ```
   Se ejecuta el instalador de Kaspersky Security Center.
3. Siga los pasos del asistente para configurar la instalación de Kaspersky Security Center.

   Cuando complete el asistente, el archivo de respuesta se modifica automáticamente de acuerdo con la nueva configuración que especificó.

## Instalación del Agente de red en modo silencioso (sin un archivo de respuesta)

Puede instalar el Agente de red con un paquete msi solo, especificando los valores de las propiedades MSI del modo estándar. Esta situación permite que el Agente de red se instale usando directivas de grupo.

No cambie el nombre del paquete de instalación Kaspersky Network Agent.msi. De lo contrario, pueden aparecer errores de instalación cuando actualice el Agente de red más adelante.

Para evitar conflictos entre los parámetros definidos mediante las propiedades MSI y los parámetros definidos en el archivo de respuesta, puede desactivar el archivo de respuesta al configurar la propiedad `DONT_USE_ANSWER_FILE=1`. El archivo MSI se encuentra en el paquete de distribución de Kaspersky Security Center, en la carpeta Packages\NetAgent\exec. Un ejemplo de una ejecución del instalador del Agente de red con un paquete msi es de la forma siguiente.

La instalación del Agente de red en modo no interactivo requiere la aceptación de los términos del Contrato de licencia de usuario final. Utilice el parámetro de `EULA=1` solo si ha leído, entendido y aceptado completamente los términos del Contrato de licencia de usuario final.

Ejemplo:

```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

También puede definir los parámetros de instalación para un paquete msi al preparar el archivo de respuesta de antemano (uno con la extensión mst). Este comando aparece de la forma siguiente:

Ejemplo:

```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

Puede especificar varios archivos de respuesta en un mismo comando.

Si desea actualizar el Agente de red con Windows Installer, ejecute el siguiente comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

## Configuración de instalación parcial a través de setup.exe

Al ejecutar la instalación de aplicaciones a través de setup.exe, puede agregar los valores de cualquier propiedad de MSI al paquete MSI.

Este comando aparece de la forma siguiente:

Ejemplo:

```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

## Parámetros de instalación del Servidor de administración

En la siguiente tabla, se describen las propiedades MSI que puede configurar al instalar el Servidor de administración. Todos los parámetros son opcionales, excepto EULA y PRIVACYPOLICY.

| Propiedad MSI | Descripción | Valores disponibles |
|---|---|---|
| EULA | Aceptación de los términos del Contrato de licencia (requerido). | • 1: he leído, comprendo y acepto en su totalidad los términos del Contrato de licencia de usuario final.<br>• Otro valor o ningún valor: no acepto los términos del Contrato de licencia (no se realizará la instalación). |
| PRIVACYPOLICY | Aceptación de los términos de la Política de privacidad (obligatorio) | • 1: entiendo y acepto que mis datos serán tratados y transmitidos (incluso a otros países) según lo descrito en la Política de privacidad. Confirmo que he leído y que comprendo en su totalidad la Política de privacidad.<br>• Otro valor o ningún valor: no acepto los términos de la Política de privacidad (no se realizará la instalación). |
| INSTALLATIONMODETYPE | Tipo de instalación del Servidor de administración | • Standard.<br>• Custom. |
| INSTALLDIR | Carpeta de instalación de la aplicación | Valor de cadena. |
| ADDLOCAL | Lista de componentes para instalar (separados por comas) | CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86.<br>Lista mínima de componentes que se requieren para instalar el Servidor de administración:<br>`ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86` |
| NETRANGETYPE | Tamaño de la red | • NRT_1_100: de 1 a 100 dispositivos.<br>• NRT_100_1000: de 101 a 1000 dispositivos.<br>• NRT_GREATER_1000: más de 1 000 dispositivos. |
| SRV_ACCOUNT_TYPE | Modo de especificar el usuario con el que funcionará el servicio del Servidor de administración | • SrvAccountDefault: la cuenta de usuario se creará automáticamente.<br>• SrvAccountUser: la cuenta de usuario se define manualmente. |
| SERVERACCOUNTNAME | Nombre de usuario para el servicio | Valor de cadena. |
| SERVERACCOUNTPWD | Contraseña del usuario para el servicio | Valor de cadena. |
| DBTYPE | Tipo de base de datos | • MySQL: se utilizará una base de datos MySQL o MariaDB.<br>• MSSQL: se usará la base de datos de Microsoft SQL Server (SQL Express). |
| MYSQLSERVERNAME | Nombre completo del servidor MySQL o MariaDB | Valor de cadena. |
| MYSQLSERVERPORT | Número de puerto para la conexión al servidor MySQL o MariaDB | Valor numérico. |
| MYSQLDBNAME | Nombre de la base de datos del servidor MySQL o MariaDB | Valor de cadena. |
| MYSQLACCOUNTNAME | Nombre de usuario para la conexión con la base de datos del servidor MySQL o MariaDB | Valor de cadena. |
| MYSQLACCOUNTPWD | Contraseña de usuario para la conexión con la base de datos del servidor MySQL o MariaDB | Valor de cadena. |
| MSSQLCONNECTIONTYPE | Tipo de uso de la base de datos MSSQL | • InstallMSSEE: instalar desde un paquete.<br>• ChooseExisting: usar un servidor instalado. |
| MSSQLSERVERNAME | Nombre completo de la instancia de SQL Server | Valor de cadena. |

| Propiedad MSI | Descripción | Valores disponibles |
|---|---|---|
| MSSQLDBNAME | Nombre de la base de datos de SQL Server | Valor de cadena. |
| MSSQLAUTHTYPE | Método de autenticación para conectarse a SQL Server | • Windows.<br>• SQLServer. |
| MSSQLACCOUNTNAME | Nombre de usuario para conectarse a SQL Server en modo SQLServer | Valor de cadena. |
| MSSQLACCOUNTPWD | Contraseña del usuario para conectarse a SQL Server en modo SQLServer | Valor de cadena. |
| CREATE_SHARE_TYPE | Forma de especificar la carpeta compartida | • Create: Crear una carpeta compartida nueva. En este caso, las propiedades siguientes se deben definir:<br>  • SHARELOCALPATH: ruta a una carpeta local.<br>  • SHAREFOLDERNAME: nombre de red de una carpeta.<br>• Nulo: se debe especificar la propiedad EXISTSHAREFOLDERNAME. |
| EXISTSHAREFOLDERNAME | Ruta completa a una carpeta compartida existente | Valor de cadena. |
| SERVERPORT | Número de puerto para conectarse al Servidor de administración | Valor numérico. |
| SERVERSSLPORT | Número de puerto para conectarse al Servidor de administración con SSL | Valor numérico. |
| SERVERADDRESS | Dirección del Servidor de administración | Valor de cadena. |
| SERVERCERT2048BITS | Tamaño de la clave para el certificado del Servidor de administración (bits) | • 1: El tamaño de la clave para el certificado del Servidor de administración es de 2048 bits.<br>• 0: el tamaño de la clave para el certificado del Servidor de administración es de 1024 bits.<br>• Si no se especifica ningún valor, el tamaño de la clave para el certificado del Servidor de administración es 2048 bits. |
| MOBILESERVERADDRESS | Dirección del Servidor de administración para la conexión de dispositivos móviles; esta propiedad se ignorará si no se ha seleccionado el componente MobileSupport | Valor de cadena. |

## Configuración de la instalación del Agente de red

La tabla a continuación describe las propiedades MSI que puede configurar al instalar el Agente de red. Todos los parámetros son opcionales, excepto SERVERADDRESS.

Propiedades de MSI

| Propiedad MSI | Descripción | Valores disponibles |
|---|---|---|
| DONT_USE_ANSWER_FILE | Lea los parámetros de instalación desde el archivo de respuesta | • 1<br>• Nulo |
| INSTALLDIR | Carpeta de instalación | |
| SERVERADDRESS | Dirección del Servidor de administración (obligatoria) | |
| SERVERPORT | Número de un puerto para la conexión al Servidor de administración | |
| SERVERSSLPORT | Número de puerto para la conexión SSL | |

| Propiedad MSI | Descripción | Valores disponibles |
|---|---|---|
| USESSL | Usar una conexión SSL o no | • 1<br>• Nulo |
| OPENUDPPORT | Abrir un puerto UDP o no | • 1<br>• Nulo |
| UDPPORT | Número de puerto UDP | |
| USEPROXY | Usar un servidor proxy o no | • 1<br>• Nulo |
| PROXYADDRESS | Dirección del servidor proxy | |
| PROXYPORT | Número de un puerto para la conexión al Servidor de administración | |
| PROXYLOGIN | Cuenta para la conexión con un servidor proxy | |
| PROXYPASSWORD | Contraseña de la cuenta para la conexión con el servidor proxy.<br><br>No especifique ningún detalle de cuentas privilegiadas en los parámetros de los paquetes de instalación. | |
| GATEWAYMODE | Modo de uso de la puerta de enlace de conexión | • 0: no usar la puerta de enlace de conexión<br>• 1: usar este Agente de red como puerta de enlace de conexión<br>• 2: conectarse al Servidor de administración mediante una puerta de enlace de conexión |
| GATEWAYADDRESS | Dirección de la puerta de enlace de conexión | |
| CERTSELECTION | Método de recibir un certificado | • GetOnFirstConnection: recibir un certificado del Servidor de administración.<br>• GetExistent: seleccionar un certificado existente. Si se selecciona esta opción, se debe definir la propiedad CERTFILE. |
| CERTFILE | Ruta al archivo de certificado | |
| VMVDI | Habilitar modo dinámico para VDI | • 1<br>• Nulo |
| LAUNCHPROGRAM | Ejecutar el servicio del Agente de red después de la instalación | • 1<br>• Nulo |

## Infraestructura virtual

Kaspersky Security Center admite el uso de máquinas virtuales. Puede instalar el Agente de red y una aplicación de seguridad en cada máquina virtual; también puede proteger todas las máquinas virtuales a nivel hipervisor. En el primer caso, las máquinas pueden protegerse con cualquier aplicación de seguridad estándar o con Kaspersky Security for Virtualization Light Agent. En el segundo caso, puede usar Kaspersky Security for Virtualization Agentless.

Kaspersky Security Center está preparado para operar con máquinas virtuales que puedan revertir su estado a un punto anterior.

## Sugerencias sobre la reducción de la carga en máquinas virtuales

Al instalar el Agente de red en una máquina virtual, le aconsejan que considere la deshabilitación de algunas funciones de Kaspersky Security Center que parecen ser de poco uso para máquinas virtuales.

Al instalar el Agente de red en una máquina virtual o en una plantilla querida para la generación de máquinas virtuales, recomendamos realizar las siguientes acciones:

- Si está ejecutando una instalación remota, en la ventana de propiedades del paquete de instalación del Agente de red, en la sección **Avanzado**, seleccione la opción **Optimizar la configuración para VDI**.
- Si está ejecutando una instalación interactiva a través de un Asistente, en la ventana Asistente, seleccione la opción **Optimizar la configuración del Agente de red para la infraestructura virtual**.

Seleccionar esas opciones cambia la configuración del Agente de red de modo que las funciones siguientes permanezcan desactivadas de forma predeterminada (antes de aplicar una directiva):

- Recopilación de información acerca del software instalado
- Recopilación de información acerca del hardware
- Recopilación de información acerca de las vulnerabilidades detectadas
- Recopilación de información acerca de las actualizaciones necesarias

Por lo general, esas funciones no son necesarias en máquinas virtuales porque usan el software uniforme y el hardware virtual.

La deshabilitación de las funciones es irreversible. Si alguna de las funciones desactivadas se requiere, la puede habilitar a través de la directiva del Agente de red, o a través de la configuración local del Agente de red. La configuración local del Agente de red está disponible a través del menú contextual del dispositivo relevante en la Consola de administración.

## Compatibilidad con máquinas virtuales dinámicas

Kaspersky Security Center es compatible con las máquinas virtuales dinámicas. Si existe una infraestructura virtual en la red de la organización, las máquinas virtuales dinámicas (temporales) se pueden utilizar en ciertos casos. Las máquinas virtuales dinámicas se crean con nombres únicos según una plantilla que preparada por el administrador. El usuario trabaja en la máquina virtual un tiempo, luego, después de apagarse, esta máquina virtual se eliminará de la infraestructura virtual. Si se ha desplegado Kaspersky Security Center en la red de la organización, se agregará una máquina virtual con el Agente de red instalado a la base de datos del Servidor de administración. Después de que desactive una máquina virtual, la entrada correspondiente también se debe eliminar de la base de datos de Servidor de administración.

Para hacer funcional la función de eliminación automática de entradas en máquinas virtuales, al instalar un Agente de red en una plantilla para máquinas virtuales dinámicas, seleccione la opción **Habilitar modo dinámico para VDI**:

- Para la instalación remota: En la ventana de propiedades del paquete de instalación del Agente de red (Sección **Avanzado**)
- Para la instalación interactiva: en el Asistente de instalación del Agente de red

Evite seleccionar la opción **Habilitar modo dinámico para VDI** al instalar el Agente de red en dispositivos físicos.

Si desea que los eventos de las máquinas virtuales dinámicas se almacenen en el Servidor de administración durante un tiempo después de eliminar esas máquinas virtuales, en la ventana de propiedades del Servidor de administración, en la sección **Repositorio de eventos**, marque la opción **Almacenar los eventos de los dispositivos eliminados** y especifique el plazo de almacenamiento máximo para los eventos (en días).

No recomendamos habilitar el cifrado de unidades en máquinas virtuales dinámicas.

### Soporte de copia de máquinas virtuales

Copiar una máquina virtual que tiene el Agente de red instalado y crear una máquina virtual a partir de una plantilla que tiene el Agente de red instalado son procedimientos idénticos al de capturar y copiar una imagen de disco duro como método para desplegar el Agente de red. Por ello, en general, si copia una máquina virtual, deberá realizar las mismas acciones que si hubiera copiado una imagen de disco para desplegar el Agente de red.

Sin embargo, los dos casos que se describen a continuación muestran el Agente de red que detecta la copia automáticamente. Debido a los motivos indicados anteriormente, no tiene que realizar las operaciones sofisticadas descritas en la sección "Despliegue con una imagen de disco duro capturada de un dispositivo":

- La opción **Habilitar modo dinámico para VDI** se seleccionó cuando el Agente de red se instaló: después de cada reinicio del sistema operativo, esta máquina virtual se reconocerá como un dispositivo nuevo, sin tener en cuenta si se ha copiado.
- Uno de los siguientes hipervisores está en uso: VMware™, HyperV® o Xen®: Agente de red detecta la copia de la máquina virtual mediante los id. modificados del hardware virtual.

El análisis de cambios en el hardware virtual no es absolutamente fiable. Antes de aplicar este método extensamente, lo debe probar en un pequeño grupo de máquinas virtuales para la versión del hipervisor actualmente usado en su organización.

## Soporte de reversión del sistema de archivos para dispositivos con Agente de red

Kaspersky Security Center es una aplicación distribuida. El revertir el sistema de archivos a un estado anterior en un dispositivo con Agente de red instalado llevará a la desincronización de datos y funcionamiento incorrecto de Kaspersky Security Center.

El sistema de archivos (o una parte de él) se puede revertir en los casos siguientes:

- Al copiar una imagen del disco duro.
- Al restaurar un estado de la máquina virtual por medio de la infraestructura virtual.
- Al restaurar datos desde una copia de seguridad o un punto de recuperación.

Las situaciones según las cuales el software de terceros en dispositivos con el Agente de red instalado afecta la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ son solo situaciones críticas para Kaspersky Security Center. Por lo tanto, siempre debe excluir esta carpeta del procedimiento de recuperación, de ser posible.

Como las reglas del lugar de trabajo de algunas organizaciones proporcionan reversiones del sistema de archivos en dispositivos, el soporte de la reversión del sistema de archivos en dispositivos con Agente de red instalado se agregó a Kaspersky Security Center a partir de la versión 10 Maintenance Release 1 (Servidor de administración y Agentes de red deben ser de la versión 10 Maintenance Release 1 o posterior). Cuando se detecta, esos dispositivos automáticamente se conectan de nuevo al Servidor de administración con limpieza de datos completa y sincronización completa.

De forma predeterminada, el soporte de la detección de reversión del sistema de archivos está habilitado en Kaspersky Security Center 15.1.

Siempre que sea posible, evite deshacer la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ en dispositivos con el Agente de red instalado, porque la resincronización completa de datos requiere una gran cantidad de recursos.

Una reversión del estado del sistema no se permite en absoluto en un dispositivo con el Servidor de administración instalado. Tampoco se aplica a la reversión de la base de datos usada por el Servidor de administración.

Puede restaurar un estado del Servidor de administración desde una copia de seguridad solo con la utilidad estándar klbackup.

# Acerca de los perfiles de conexión para los usuarios fuera de la oficina

Los usuarios de computadoras portátiles fuera de la oficina (más adelante también llamadas "dispositivos") tal vez tengan que cambiar el método de conexión a un Servidor de administración o entre Servidores de administración, según la ubicación actual del dispositivo en la red de la empresa.

Los perfiles de conexión solo son compatibles con dispositivos que ejecutan Windows y MacOS.

## Utilización de direcciones diferentes de un Servidor de administración solo

Los dispositivos con Agente de red instalado pueden conectarse al Servidor de administración desde la red interna de la organización o desde Internet. Esta situación puede requerir que el Agente de red use direcciones diferentes para la conexión con el Servidor de administración: dirección externa del Servidor de administración para conexión a Internet y dirección interna del Servidor de administración para la conexión a la red interna.

Para hacer esto, debe agregar un perfil (para la conexión con el Servidor de administración desde Internet) a la directiva del Agente de red. Añada el perfil en las propiedades de la directiva (sección **Conectividad**, subsección **Perfiles de conexión**). En la ventana de creación de perfil, debe deshabilitar la opción **Usar para recibir actualizaciones solamente** y seleccionar la opción **Sincronizar configuración de conexión con la configuración del Servidor de administración especificada en este perfil**. Si usa una puerta de enlace de conexión para acceder al Servidor de administración (por ejemplo, en una configuración de Kaspersky Security Center como la que se describe en Acceso a Internet: Agente de red como puerta de enlace de conexión en una DMZ), debe especificar la dirección de la puerta de enlace de conexión en el campo correspondiente del perfil de conexión.

### Conmutación entre Servidores de administración según la red actual

Si la organización tiene varias oficinas con Servidores de administración diferentes y algunos dispositivos con Agentes de red instalados se transfieren entre ellos, necesita un Agente de red para conectarse al Servidor de administración de la red local en la oficina donde el dispositivo se localiza actualmente.

En este caso, debe crear un perfil para la conexión con el Servidor de administración en las propiedades de la directiva del Agente de red para cada una de las oficinas, excepto la oficina local donde el Servidor de administración doméstico se encuentra localizado. Debe especificar las direcciones de los Servidores de administración en perfiles de conexión y habilitar o deshabilitar la opción **Usar para recibir actualizaciones solamente**:

- Habilite la opción si necesita que el Agente de red se sincronice con el Servidor de administración doméstico mientras usa el Servidor local para descargar actualizaciones únicamente.
- Deshabilite la opción si es necesario para que el Agente de red sea administrado completamente por el Servidor de administración local.

Después de esto, debe configurar las condiciones de conmutación para los perfiles recién creados: al menos una condición para cada una de las oficinas, excepto la oficina local. El propósito de cada condición consiste en la detección de elementos que son específicos para el entorno de la red de una oficina. Si una condición es verdadera, el perfil correspondiente se activa. Si ninguna de las condiciones es verdadera, el Agente de red cambia al Servidor de administración doméstico.

# Despliegue de la característica Administración de dispositivos móviles

Esta sección proporciona información que le permitirá poner en funcionamiento la característica Administración de dispositivos móviles.

## Conexión de dispositivos KES al Servidor de administración

Kaspersky Device Management for iOS es compatible con dos esquemas o modos de conectar los dispositivos KES al Servidor de administración:

- Esquema en el que los dispositivos se conectan en forma directa al Servidor de administración
- Esquema de despliegue que involucra un proxy inverso compatible con la delegación restringida de Kerberos

## Conexión directa de dispositivos al Servidor de administración

Los dispositivos KES pueden conectarse directamente al puerto 13292 del Servidor de administración.

Según el método usado para la autenticación, dos opciones son posibles para la conexión de dispositivos KES al Servidor de administración:

- Conectar dispositivos con un certificado cliente (certificado de usuario)
- Conectar dispositivos sin un certificado cliente (certificado de usuario)

### Conectar un dispositivo con un certificado cliente (certificado de usuario)

Al conectar un dispositivo con un certificado cliente (certificado de usuario), ese dispositivo está asociado a la cuenta de usuario a la cual el certificado correspondiente se ha asignado a través de herramientas del Servidor de administración.

En este caso, se utilizará la autenticación SSL bidireccional (autenticación mutua). Tanto el Servidor de administración como el dispositivo serán autenticados con certificados.

### Conectar un dispositivo sin un certificado cliente (certificado de usuario)

Al conectar un dispositivo sin un certificado cliente (certificado de usuario), ese dispositivo no está asociado a ninguna de las cuentas de usuario en el Servidor de administración. Pero cuando el dispositivo reciba un certificado, este dispositivo se vinculará al usuario al que el Servidor de administración le haya asignado el certificado correspondiente.

Al conectar ese dispositivo al Servidor de administración, la Autenticación SSL unidireccional se aplicará, lo que significa que solo el Servidor de administración se autentica con el certificado. Después de que el dispositivo reciba el certificado cliente (certificado de usuario), el tipo de autenticación cambiará a la autenticación SSL bidireccional (autenticación SSL de 2 modos, autenticación mutua).

## Esquema para conectar dispositivos KES al Servidor en el que se usa la delegación restringida de Kerberos (KCD)

El esquema para conectar dispositivos KES al Servidor de administración utilizando la delegación restringida de Kerberos (KCD) permite lo siguiente:

- Integración con un proxy inverso compatible con KCD.
- Uso de la delegación restringida de Kerberos (denominado en lo sucesivo KCD) para la autenticación de dispositivos móviles.
- Integración con una infraestructura de claves públicas (denominada, en lo sucesivo, PKI) para aplicar certificados de usuario.

Al usar este esquema de distribución, tenga en cuenta lo siguiente:

- El tipo de conexión de dispositivos KES al proxy inverso debe ser la "autenticación SSL bidireccional", es decir, un dispositivo debe conectarse al proxy inverso a través de su certificado de usuario de propiedad. Para hacer esto, tiene que integrar el certificado cliente (certificado de usuario) en el paquete de instalación de Kaspersky Endpoint Security para Android, que se ha instalado en el dispositivo. Este paquete KES debe ser creado por el Servidor de administración expresamente para este dispositivo (usuario).

- Debe especificar el certificado (personalizado) especial en vez del certificado del servidor predeterminado para el protocolo móvil:

  1. En la ventana de Propiedades del Servidor de administración, en la sección **Configuración**, seleccione la casilla **Abrir puerto para dispositivos móviles** y seleccione **Agregar certificado** en la lista desplegable.

  2. En la ventana que se abre, especifique el mismo certificado que se configuró en el proxy inverso cuando el punto de acceso al protocolo móvil se publicó en el Servidor de administración.

- Los certificados de usuario para dispositivos KES deben ser emitidos por la Entidad de certificación (CA) del dominio. Tenga en cuenta que si el dominio incluye varias CA originales, los certificados de usuario deben ser emitidos por la CA que se haya configurado en la publicación del proxy inverso.

  Se puede asegurar de que el certificado cliente (certificado de usuario) cumpla con el requisito descrito anteriormente usando uno de los métodos siguientes:

  - Especifique el certificado de usuario especial en el Asistente de nuevo paquete y en el Asistente de instalación de certificados.

  - Integre el Servidor de administración con PKI del dominio y defina el parámetro correspondiente en las reglas para la emisión de certificados:

    1. En el árbol de consola, expanda la carpeta **Administración de dispositivos móviles** y seleccione la subcarpeta **Certificados**.

    2. En el espacio de trabajo de la carpeta **Certificados**, haga clic en el botón **Configurar reglas de emisión de certificados** para abrir la ventana **Reglas de emisión de certificados**.

    3. En la sección **Integración con PKI**, configure la integración con la Infraestructura de clave pública.

    4. En la sección **Emisión de certificados para dispositivos móviles**, especifique el origen de los certificados.

A continuación se muestra un ejemplo de instalación de la delegación restringida de Kerberos (KCD) con las siguientes suposiciones:

- El punto del acceso al protocolo móvil en el Servidor de administración está configurado en el puerto 13292.

- El nombre del dispositivo con el proxy inverso es firewall.mydom.local.

- El nombre del dispositivo con el Servidor de administración es ksc.mydom.local.

- El Nombre de la publicación externa del punto de acceso al protocolo móvil es kes4mob.mydom.global.

## Cuenta del dominio para el Servidor de administración

Debe crear una cuenta de dominio (por ejemplo, KSCMobileSrvcUsr) bajo la cual se ejecutará el servicio del Servidor de administración. Puede especificar una cuenta para el servicio del Servidor de administración al instalar el Servidor de administración o a través de la utilidad klsrvswch. La utilidad klsrvswch se localiza en la carpeta de instalación del Servidor de administración. La ruta de instalación predeterminada: <Disk>:\Archivos de programa (x86)\Kaspersky Lab\Kaspersky Security Center.

Una cuenta de dominio debe ser especificada por las siguientes razones:

- La función para la administración de dispositivos KES es una parte integral del Servidor de administración.
- Para asegurar un correcto funcionamiento de la delegación restringida de Kerberos (KCD), el lado de recepción (por ej., el Servidor de administración) se debe ejecutar bajo una cuenta de dominio.

## Nombre principal del servicio para http/kes4mob.mydom.local

En el dominio, bajo la cuenta KSCMobileSrvcUsr, agregue un SPN para publicar el servicio del protocolo móvil en el puerto 13292 del dispositivo con el Servidor de administración. Para el dispositivo kes4mob.mydom.local con el Servidor de administración, esto aparecerá de la forma siguiente:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

## Configuración de las propiedades del dominio del dispositivo con el proxy inverso (firewall.mydom.local)

Para delegar el tráfico, delegue el dispositivo con el proxy inverso (firewall.mydom.local) al servicio que es definido por SPN (http/iosmdm.mydom.local).

*Para delegar el dispositivo con el proxy inverso al servicio definido por SPN (http/iosmdm.mydom.local), el administrador debe realizar las siguientes acciones:*

1. En el complemento de Microsoft Management Console denominado "Usuarios y equipos de Active Directory", seleccione el dispositivo con el proxy inverso instalado (firewall.mydom.local).
2. En las propiedades del dispositivo, en la pestaña **Delegación**, configure la opción **Confiar este equipo para delegación para un servicio especificado únicamente** en **Usar cualquier protocolo de autenticación**.
3. En los **Servicios en los cuales esta cuenta puede presentar credenciales delegada**, agregue SPN http/kes4mob.mydom.local:13292.

## Certificado especial (personalizado) para la publicación (kes4mob.mydom.global)

Para publicar el protocolo móvil del Servidor de administración, debe emitir un certificado (personalizado) especial para FQDN kes4mob.mydom.global y especificarlo en vez del certificado del servidor predeterminado en la configuración del protocolo móvil del Servidor de administración en la Consola de administración. Para hacerlo, en la ventana de propiedades del Servidor de administración, en la sección **Configuración**, seleccione la casilla **Abrir puerto para dispositivos móviles** y luego seleccione **Agregar certificado** en la lista desplegable.

Tenga en cuenta que el contenedor del certificado del servidor (el archivo con la extensión p12 o pfx) también debe contener una cadena de certificados raíz (claves públicas).

## Configuración de la publicación en el proxy inverso

En el proxy inverso, para el tráfico que va desde un dispositivo móvil al puerto 13292 de kes4mob.mydom.global, tiene que configurar KCD en SPN (http/kes4mob.mydom.local:13292) usando el certificado del servidor emitido para FQND (kes4mob.mydom.global). Tenga en cuenta que la publicación y el punto de acceso publicado (puerto 13292 del Servidor de administración) deben compartir el mismo certificado del servidor.

## Usar Firebase Cloud Messaging

Para asegurar la distribución a tiempo de los comandos a los dispositivos KES administrados por el sistema operativo Android, Kaspersky Security Center utiliza el mecanismo de notificaciones push. Las notificaciones push se intercambian entre los dispositivos KES y el Servidor de administración a través de Firebase Cloud Messaging (en adelante, FCM). En la Consola de administración de Kaspersky Security Center, puede especificar la configuración de Firebase Cloud Messaging para conectar los dispositivos KES al servicio.

Para recuperar la configuración de Firebase Cloud Messaging, debe tener una cuenta de Google.

*Para habilitar el uso de FCM:*

1. En la Consola de administración, seleccione el nodo **Administración de dispositivos móviles** y la carpeta **Dispositivos móviles**.
2. En el menú contextual de la carpeta **Dispositivos móviles**, seleccione **Propiedades**.
3. En las propiedades de la carpeta, seleccione la sección **Configuración de Firebase Cloud Messaging**.
4. En el campo **Número de proyecto de Firebase**, especifique el Id. del remitente de FCM.
5. En el campo **Archivo de clave privada (en formato JSON)**, seleccione el archivo de clave privada.

   En la próxima sincronización con el Servidor de administración, los dispositivos KES administrados por sistemas operativos Android estarán conectados a Firebase Cloud Messaging.

Puede editar la configuración de Firebase Cloud Messaging al hacer clic en el botón **Restablecer configuración**.

Cuando cambia a otro proyecto de Firebase, debe esperar 10 minutos para que FCM reanude su ejecución.

El servicio de FCM opera en los siguientes intervalos de direcciones:

- Desde el lado del dispositivo KES, el acceso se requiere para los puertos 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) y 5230 (HTTPS) de las direcciones siguientes:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Todas las direcciones IP incluidas en el ASN 15169, perteneciente a Google
- Del lado del Servidor de administración, se requiere acceso al puerto 443 (HTTPS) de las siguientes direcciones:
  - fcm.googleapis.com
  - Todas las direcciones IP incluidas en el ASN 15169, perteneciente a Google

Si la configuración del servidor proxy (**Avanzado**/**Configuración de acceso a Internet**) se ha especificado en las propiedades del Servidor de administración en la Consola de administración, se utilizarán para la interacción con FCM.

## Configuración de FCM: obtener el Id. del remitente y el archivo de clave privada

*Para configurar FCM:*

1. Regístrese en el portal de Google.
2. Vaya a la consola de Firebase.
3. Realice una de las siguientes acciones:
   - Para crear un nuevo proyecto, haga clic en **Crear un proyecto** y siga las instrucciones en pantalla.
   - Abra un proyecto existente.
4. Haga clic en el ícono de ajustes y seleccione **Configuración del proyecto**.
   Se abre la ventana **Configuración del proyecto**.
5. Seleccione la pestaña **Cloud Messaging**.
6. Recupere el id. del remitente correspondiente del campo **Id. del remitente** en la sección **API de Firebase Cloud Messaging (V1)**.
7. Seleccione la pestaña **Cuentas de servicio** y haga clic en **Generar nueva clave privada**.
8. En la ventana que se abre, haga clic en **Generar clave** para generar y descargar un archivo de clave privada.

Firebase Cloud Messaging queda configurado.

# Integración con una infraestructura de claves públicas

La integración con la infraestructura de claves públicas (denominada en lo sucesivo PKI) se creó principalmente para simplificar la emisión de certificados de usuario del dominio por el Servidor de administración.

El administrador puede asignar un certificado de dominio para un usuario en la Consola de administración. Esto se puede hacer usando uno de los siguientes métodos:

- Asigne al usuario un certificado especial (personalizado) desde un archivo en el Asistente de instalación de certificados.
- Realice la integración con PKI y asigne PKI para que actúe como origen de certificados para un tipo concreto de certificados o para todos los tipos de certificados.

La configuración de integración con PKI está disponible en el espacio de trabajo de la carpeta **Administración de dispositivos móviles** / / **Certificados** al hacer clic en el enlace **Integrar con infraestructura de claves públicas**.

## Principio general de integración con PKI para emisión de certificados de usuario del dominio

En la Consola de administración, haga clic en el enlace **Integrar con infraestructura de claves públicas** en el espacio de trabajo de la carpeta **Administración de dispositivos móviles** / **Certificados** para especificar una cuenta de dominio que utilizará el Servidor de administración para emitir certificados de usuario del dominio a través de las CA del dominio (denominado en lo sucesivo la cuenta mediante la cual se realiza la integración con PKI).

Tenga en cuenta lo siguiente:

- La configuración de integración con PKI le proporciona la posibilidad de especificar la plantilla predeterminada para todos los tipos de certificados. Tenga en cuenta que las reglas para la emisión de certificados (disponibles en el espacio de trabajo de la carpeta **Administración de dispositivos móviles** / **Certificados**, al hacer clic en el botón **Configurar reglas de emisión de certificados**), le permiten especificar una plantilla individual para cada tipo de certificados.
- Un certificado especial del Agente de inscripción (EA) se debe instalar en el dispositivo con el Servidor de administración, en el repositorio de certificados de la cuenta bajo la cual la integración con PKI se realiza. El certificado del Agente de inscripción (EA) es emitido por el administrador del CA del dominio (Entidad de certificación).

La cuenta bajo la cual la integración con PKI se realiza debe cumplir los criterios siguientes:

- Es un usuario de dominio.
- Es un administrador local del dispositivo con el Servidor de administración desde el cual la integración con PKI se inicia.
- Tiene derecho a *Iniciar sesión como servicio*.
- El dispositivo con el Servidor de administración instalado se debe ejecutar al menos una vez bajo esta cuenta para crear un perfil de usuario permanente.

## Servidor web de Kaspersky Security Center

Servidor web de Kaspersky Security Center (denominado en lo sucesivo Servidor web) es un componente de Kaspersky Security Center. El Servidor web está diseñado para publicar paquetes de instalación independientes, paquetes de instalación independientes para dispositivos móviles y archivos de la carpeta compartida.

Los paquetes de instalación creados se publican en el Servidor web automáticamente y se eliminan después de la primera descarga. El administrador puede enviar el nuevo enlace al usuario de cualquier manera que le resulte conveniente (por ejemplo, por correo electrónico).

Al hacer clic en este enlace, el usuario puede descargar la información solicitada a un dispositivo móvil.

### Configuración del Servidor web

Si necesita ajustar los parámetros del Servidor web, puede modificar sus propiedades para cambiar los puertos utilizados para HTTP (8060) y HTTPS (8061). Además de cambiar los puertos, puede reemplazar el certificado HTTPS del Servidor y cambiar el nombre de dominio (FQDN) utilizado por el Servidor web para el acceso mediante HTTP.

# Otro trabajo de rutina

Esta sección proporciona recomendaciones sobre el trabajo rutinario con Kaspersky Security Center.

# Controlar los semáforos y los eventos registrados en la Consola de Administración

La Consola de administración le permite evaluar rápidamente el estado actual de Kaspersky Security Center y dispositivos administrados al comprobar los semáforos. Los semáforos se muestran en el espacio de trabajo del nodo **Servidor de administración**, en la pestaña **Supervisión**. La pestaña proporciona seis paneles de información con semáforos y eventos registrados. Un semáforo es una barra vertical de color en el lado izquierdo de un panel. Cada panel con un semáforo equivale a un alcance funcional específico de Kaspersky Security Center (ver la tabla a continuación).

Alcances cubiertos por semáforos en la Consola de administración

| Nombre del panel | Alcance del semáforo |
|---|---|
| **Despliegue** | Instalación del Agente de red y aplicaciones de seguridad en dispositivos en una red de la organización |
| **Esquema de administración** | Estructura de grupos de administración. Análisis de la red. Reglas de movimiento de dispositivos |
| **Opciones de protección** | Funcionalidad de la aplicación de seguridad: estado de la protección, análisis del malware |
| **Actualización** | Actualizaciones y parches |
| **Supervisión** | Estado de protección |
| **Servidor de administración** | Funciones y propiedades del Servidor de administración |

Cada semáforo puede prenderse en cualquiera de estos cinco colores (ver la tabla a continuación). El color de un semáforo depende del estado actual de Kaspersky Security Center y de los eventos que se registraron.

Códigos de colores de los semáforos

| Estado | Color del semáforo | Significado del color del semáforo |
|---|---|---|
| Informativo | Verde | No se requiere intervención del administrador. |
| Advertencia | Amarillo | Se requiere intervención del administrador. |
| Crítico | Rojo | Se han detectado graves problemas. Intervención del administrador requerida para solucionarlos. |
| Informativo | Azul claro | Se han registrado eventos que no están relacionados con amenazas posibles o reales a la seguridad de dispositivos administrados. |
| Informativo | Gris | Los detalles de eventos no están disponibles o todavía no se han recuperado. |

El objetivo del administrador es mantener los semáforos en todos los paneles de información en la pestaña **Supervisión** en verde.

Los paneles de información también muestran los eventos registrados que afectan los semáforos y el estado de Kaspersky Security Center (vea la siguiente tabla).

Nombre, descripción y color de semáforo de los eventos registrados

| Color del semáforo | Nombre que se muestra para el tipo de evento | Tipo de evento | Descripción |
|---|---|---|---|
| Rojo | **La licencia caducó en %1 dispositivo(s)** | IDS_AK_STATUS_LIC_EXPAIRED | Este tipo de eventos ocurre cuando caduca la licencia comercial.<br>Kaspersky Security Center verifica una vez al día si la licencia ha caducado en los dispositivos.<br>Cuando caduca la licencia comercial, Kaspersky Security Center solo brinda acceso a las funciones básicas.<br>Para seguir usando Kaspersky Security Center, renueve su licencia comercial. |
| Rojo | **La aplicación de seguridad no se está ejecutando en %1 dispositivo(s)** | IDS_AK_STATUS_AV_NOT_RUNNING | Este tipo de evento ocurre cuando la aplicación de seguridad instalada en el dispositivo no se está ejecutando.<br>Asegúrese de que Kaspersky Endpoint Security se esté ejecutando en el dispositivo. |
| Rojo | **La protección está deshabilitada en: %1 dispositivo(s)** | IDS_AK_STATUS_RTP_NOT_RUNNING | Este tipo de evento ocurre cuando la aplicación de seguridad del dispositivo ha estado deshabilitada por un tiempo superior al especificado.<br>Revise el estado de la protección en tiempo real en el dispositivo y asegúrese de que todos los componentes de protección que necesite estén habilitados. |
| Rojo | **Se detectó una vulnerabilidad de software en los dispositivos** | IDS_AK_STATUS_VULNERABILITIES_FOUND | Este tipo de evento ocurre cuando la tarea *Buscar vulnerabilidades y actualizaciones requeridas* ha detectado vulnerabilidades con el nivel de gravedad especificado en las aplicaciones instaladas en el dispositivo.<br>Consulte la lista de actualizaciones disponibles en la subcarpeta **Actualizaciones de software** de la carpeta **Administración de aplicaciones**. Esta carpeta contiene una lista de las actualizaciones obtenidas por el Servidor de administración para las aplicaciones de Microsoft y para los productos de otros proveedores de software que pueden distribuirse a los dispositivos.<br>Tras revisar la información sobre las actualizaciones disponibles, instálelas en el dispositivo. |
| Rojo | **Se han registrado eventos críticos en el Servidor de administración** | IDS_AK_STATUS_EVENTS_OCCURED | Este tipo de evento ocurre cuando se detectan eventos críticos del Servidor de administración.<br>Revise la lista de eventos almacenados en el Servidor de administración y luego corrija los eventos críticos uno por uno. |

| Color del semáforo | Nombre que se muestra para el tipo de evento | Tipo de evento | Descripción |
|---|---|---|---|
| Rojo | **Eventos de error registrados en el Servidor de administración** | IDS_AK_STATUS_ERROR_EVENTS_OCCURED | Este tipo de evento ocurre cuando se registran errores inesperados en el lado del Servidor de administración.<br>Revise la lista de eventos almacenados en el Servidor de administración y luego corrija los errores uno por uno. |
| Rojo | **Se perdió la conexión con %1 dispositivo(s)** | IDS_AK_STATUS_ADM_LOST_CONTROL1 | Este tipo de evento ocurre cuando se pierde la conexión entre el Servidor de administración y el dispositivo.<br>Revise la lista de dispositivos desconectados e intente volver a conectarlos. |
| Rojo | **%1 dispositivo/s no se ha conectado al Servidor de administración en mucho tiempo** | IDS_AK_STATUS_ADM_NOT_CONNECTED1 | Este tipo de evento ocurre cuando el dispositivo se encuentra apagado y, debido a ello, no se ha conectado al Servidor de administración en el período de tiempo especificado.<br>Asegúrese de que el dispositivo esté encendido y compruebe que el Agente de red se esté ejecutando. |
| Rojo | **Hay %1 dispositivo(s) cuyo estado no es Sin inconvenientes** | IDS_AK_STATUS_HOST_NOT_OK | Este tipo de evento ocurre cuando el estado *Sin inconvenientes* del dispositivo conectado al Servidor de administración cambia a *Crítico* o a *Advertencia*.<br>Puede buscar una solución a este problema con la Utilidad de diagnóstico remoto de Kaspersky Security Center. |
| Rojo | **Las bases de datos están desactualizadas en: %1 dispositivo(s)** | IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED | Este tipo de evento ocurre cuando las bases de datos antivirus no se han actualizado en el dispositivo dentro del intervalo de tiempo especificado.<br>Siga las instrucciones para actualizar las bases de datos de Kaspersky. |
| Rojo | **Dispositivo/s donde no se ha realizado una comprobación de actualizaciones de Windows Update en mucho tiempo: %1** | IDS_AK_STATUS_WUA_DATA_OBSOLETE | Este tipo de evento ocurre cuando la tarea *Realizar la sincronización con Windows Update* no se ha ejecutado en el intervalo de tiempo especificado.<br>Siga las instrucciones para sincronizar las actualizaciones de Windows Update con el Servidor de administración. |
| Rojo | **Es necesario instalar %1 complemento(s) para Kaspersky Security Center** | IDS_AK_STATUS_PLUGINS_REQUIRED2 | Este tipo de evento ocurre cuando se deben instalar complementos adicionales para las aplicaciones de Kaspersky.<br>Descargue e instale los complementos de administración necesarios para la aplicación Kaspersky desde la página web del Servicio de soporte técnico de Kaspersky. |

# Acceso remoto a dispositivos administrados

Esta sección proporciona información sobre el acceso remoto a dispositivos administrados.

# Uso de la opción "No desconectarse del Servidor de administración" para proporcionar conectividad continua entre un dispositivo administrado y el Servidor de administración

Si usted no utiliza servidores push, Kaspersky Security Center no proporciona conectividad continua entre los dispositivos administrados y el Servidor de administración. Los Agentes de red en los dispositivos administrados periódicamente establecen conexiones y se sincronizan con el Servidor de administración. El intervalo entre esas sesiones de sincronización se define en una directiva del Agente de red. Si se requiere una sincronización temprana, el Servidor de administración (o un punto de distribución, si está en uso) envía un paquete de red firmado a través de una red IPv4 o IPv6 al puerto UDP del Agente de red. El puerto por defecto es el 15000. Si ninguna conexión a través de UDP es posible entre el Servidor de administración y un dispositivo administrado, la sincronización se ejecutará en la siguiente conexión regular del Agente de red al Servidor de administración dentro del intervalo de sincronización.

Algunas operaciones no se pueden realizar sin una conexión temprana entre el Agente de red y el Servidor de administración, como ejecutar y detener tareas locales, recibir estadísticas para una aplicación administrada o crear un túnel. Para resolver este problema, si no utiliza servidores push, puede usar la opción **No desconectar del Servidor de administración** para garantizar conectividad continua entre el dispositivo administrado y el Servidor de administración.

*Para proporcionar conexión continua entre un dispositivo administrado y el Servidor de administración:*

1. En el árbol de consola, seleccione la carpeta **Dispositivos administrados**.
2. En el espacio de trabajo de la carpeta, seleccione el dispositivo administrado con el que desea proporcionar conectividad continua.
3. En el menú contextual del dispositivo, seleccione **Propiedades**.

   Se abre la ventana de propiedades del dispositivo seleccionado.
4. En la sección **General** de la ventana, seleccione la opción **No desconectar del Servidor de administración**.

Hay una conexión continua establecida entre el dispositivo administrado y el Servidor de administración.

El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

# Acerca de la comprobación de la hora de conexión entre un dispositivo y el Servidor de administración

Cuando se apaga un dispositivo, el Agente de red notifica el Servidor de administración de este evento. En la Consola de administración, ese dispositivo se muestra como apagado. Sin embargo, el Agente de red no puede notificar el Servidor de administración de todos los eventos de este tipo. El Servidor de administración, por lo tanto, periódicamente analiza el atributo **Conectado al Servidor de administración** (el valor de este atributo se muestra en la Consola de administración, en las propiedades del dispositivo, en la sección **General**) para cada dispositivo y lo compara con el intervalo de sincronización de la configuración actual del Agente de red. Si un dispositivo no ha respondido durante más de tres intervalos de sincronización sucesivos, ese dispositivo se marca como apagado.

## Acerca de la sincronización forzada

Aunque Kaspersky Security Center automáticamente sincroniza el estado, la configuración, las tareas y las directivas para dispositivos administrados, en algunos casos el administrador tiene que saber exactamente si la sincronización se ha realizado ya para un dispositivo especificado en este momento.

En el menú contextual de dispositivos administrados en la Consola de administración, el elemento de menú **Todas las tareas** contiene el comando **Forzar sincronización**. Cuando Kaspersky Security Center 15.1 ejecuta este comando, el Servidor de administración intenta conectarse con el dispositivo seleccionado. Si la conexión se establece, se realiza una sincronización forzada en ese momento. Si la comunicación no puede establecerse, la sincronización forzada se pospone hasta la siguiente conexión programada entre el Agente de red y el Servidor de administración.

## Sobre la tunelización

Kaspersky Security Center permite hacer túneles de conexión TCP desde la Consola de administración mediante el Servidor de administración y luego mediante el Agente de red a un puerto especificado en un dispositivo administrado. Gracias a este túnel, una aplicación cliente instalada en el mismo dispositivo que la Consola de administración puede conectarse a un puerto TCP de un dispositivo administrado incluso si no existe una vía de conexión directa entre la Consola de administración y ese dispositivo administrado.

Por ejemplo, los túneles se utilizan para establecer conexiones con un escritorio remoto, tanto para conectarse a una sesión existente, como para crear una sesión remota nueva.

También se pueden habilitar con herramientas externas. Por ejemplo, el administrador puede ejecutar la utilidad PuTTY, el cliente VNC y otras herramientas de esta manera.

# Guía de dimensionamiento

Esta sección proporciona información sobre el dimensionamiento de Kaspersky Security Center.

## Acerca de esta Guía

La Guía de dimensionamiento de Kaspersky Security Center 15.1 (también denominada "Kaspersky Security Center") está orientada a los profesionales que instalan y administran Kaspersky Security Center, así como también a aquellos que ofrecen Servicio de soporte técnico a las organizaciones que usan Kaspersky Security Center.

Todas las recomendaciones y evaluaciones se dan para las redes en las que Kaspersky Security Center administra la protección de dispositivos que tengan instalado el software de Kaspersky, incluidos los dispositivos móviles. Si los dispositivos móviles o cualquier otro dispositivo administrado, se deben considerar por separado, esto se establece específicamente.

Para obtener y mantener un rendimiento óptimo en diferentes condiciones operativas, debe tener en cuenta la cantidad de dispositivos en red, la topología de red y el conjunto de funciones de Kaspersky Security Center que necesita.

Esta Guía proporciona la siguiente información:

- Limitaciones de Kaspersky Security Center
- Evaluaciones para los nodos clave de Kaspersky Security Center (Servidores de administración y puntos de distribución):
  - Requisitos de hardware para Servidores de administración y puntos de distribución
  - Evaluación del número y la jerarquía de los Servidores de administración
  - Cálculo del número y la configuración de los puntos de distribución
- Configuración del registro de eventos en la base de datos según el número de dispositivos en red
- Prácticas recomendadas habituales para la optimización del Prácticas recomendadas comunes para optimizar el rendimiento
- Configuración de tareas específicas destinadas a un rendimiento óptimo de Kaspersky Security Center
- Tasa de tráfico (carga de red) entre el Servidor de administración de Kaspersky Security Center y cada dispositivo protegido

Se recomienda consultar esta guía en los siguientes casos:

- Al planear recursos antes de la instalación de Kaspersky Security Center
- Al planear cambios significativos en la escala de la red en la que se implementa Kaspersky Security Center

- Al dejar de utilizar Kaspersky Security Center dentro de un segmento de red limitado (un entorno de prueba) y cambiar al despliegue en gran escala de Kaspersky Security Center en la red corporativa
- Al realizar cambios en el conjunto de funciones de Kaspersky Security Center utilizadas

# Información sobre las limitaciones de Kaspersky Security Center

La tabla siguiente muestra las limitaciones de la versión actual de Kaspersky Security Center.

Limitaciones de Kaspersky Security Center

| Tipo de limitación | Valor |
|---|---|
| Número máximo de dispositivos administrados por Servidor de administración | 100000 |
| Número máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada | 300 |
| Número máximo de grupos de administración | 10000 |
| Número máximo de eventos para almacenar | 45 000 000 |
| Número máximo de directivas | 2000 |
| Número máximo de tareas | 2000 |
| Número total máximo de objetos de Active Directory (unidades organizativas [OU] y cuentas de usuarios, dispositivos y grupos de seguridad) | 1 000 000 |
| Número máximo de perfiles en una directiva | 100 |
| Número máximo de Servidores de administración secundarios en un solo Servidor de administración principal | 500 |
| Número máximo de Servidores de administración virtual | 500 |
| Número máximo de dispositivos que un único punto de distribución puede abarcar (los puntos de distribución pueden abarcar únicamente dispositivos no móviles) | 10000 |
| Número máximo de dispositivos que pueden usar una única puerta de enlace de conexión | 10 000, incluidos los dispositivos móviles |
| Número máximo de dispositivos móviles por Servidor de administración | 100 000 menos el número de dispositivos administrados inmóviles |

# Evaluaciones para Servidores de administración

Esta sección proporciona los requisitos de software y hardware para los dispositivos utilizados como Servidores de administración. También se proporcionan recomendaciones para calcular el número y la jerarquía de los Servidores de administración según la configuración de la red de la organización.

## Evaluación de recursos del hardware para el Servidor de administración

Esta sección contiene evaluaciones que proporcionan una guía para planificar recursos de hardware para el Servidor de administración. Se proporciona una recomendación sobre la evaluación del espacio en disco cuando se utiliza la función de administración de vulnerabilidades y parches por separado.

# Requisitos de hardware para DBMS y el Servidor de administración

Las siguientes tablas proporcionan información sobre los requisitos de hardware mínimos (obtenidos durante pruebas) para DBMS y el Servidor de administración. Para ver una lista completa de los sistemas operativos y de los DBMS admitidos, consulte la lista de requisitos de hardware y software.

## El Servidor de administración y el DBMS están en dispositivos diferentes, la red incluye 50 000 dispositivos

Configuración del dispositivo con el Servidor de administración instalado

| Hardware | Valor |
|---|---|
| CPU | 4 núcleos, 2500 MHz |
| RAM | 8 GB |
| Disco duro | 300 GB, RAID recomendado |
| Adaptador de red | 1 Gbit |

La configuración del dispositivo que tiene DBMS instalado

| Hardware | Valor |
|---|---|
| CPU | 4 núcleos, 2500 MHz |
| RAM | 16 GB |
| Disco duro | 200 GB, SATA RAID |
| Adaptador de red | 1 Gbit |

## El Servidor de administración y DBMS están en el mismo dispositivo, la red incluye 50 000 dispositivos

La configuración del dispositivo que tiene el Servidor de administración y DBMS instalados

| Hardware | Valor |
|---|---|
| CPU | 8 núcleos, 2500 MHz |
| RAM | 16 GB |
| Disco duro | 500 GB, SATA RAID |
| Adaptador de red | 1 Gbit |

## El Servidor de administración y el DBMS están en dispositivos diferentes, la red incluye 100 000 dispositivos

Configuración del dispositivo con el Servidor de administración instalado

| Hardware | Valor |
|---|---|
| CPU | 8 núcleos, 2.13 GHz |
| RAM | 8 GB |
| Disco duro | 1 TB, con RAID |
| Adaptador de red | 1 Gbit |

Configuración del dispositivo con DBMS instalado

| Hardware | Valor |
|---|---|
| CPU | 8 núcleos, 2,53 GHz |
| RAM | 26 GB |
| Disco duro | 500 GB, SATA RAID |
| Adaptador de red | 1 Gbit |

Las pruebas se ejecutaron con la configuración siguiente:

- La asignación automática de puntos de distribución está habilitada en el Servidor de administración, o los puntos de distribución se asignan manualmente de acuerdo con la tabla recomendada.
- La tarea de copia de seguridad guarda copias de seguridad en un recurso del archivo localizado en un servidor dedicado.
- El intervalo de sincronización para Agentes de red está configurado según lo especificado en la tabla a continuación.

  Intervalo de sincronización para Agentes de red

  | Intervalo de sincronización (minutos) | Número de dispositivos administrados |
  |---|---|
  | 15 | 10000 |
  | 30 | 20000 |
  | 45 | 30000 |
  | 60 | 40000 |
  | 75 | 50000 |
  | 150 | 100000 |

## Evaluación de espacio de la base de datos

La fórmula siguiente permite calcular de manera aproximada la cantidad de espacio que debe reservarse en la base de datos:

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

donde:

- C es el número de dispositivos
- E es el número de eventos que se almacenan
- A es el número total de objetos de Active Directory:
  - Cuentas del dispositivo
  - Cuentas de usuario
  - Cuentas de grupos de seguridad
  - Unidades de organización de Active Directory

  Si el análisis de Active Directory se encuentra deshabilitado, A se considera igual a cero.

- N es la cantidad promedio de archivos ejecutables que se incluyen en el inventario de un dispositivo de endpoint.

- F es el número de dispositivos de endpoint, donde se incluye en el inventario de los archivos ejecutables.

Si planea habilitar (en la configuración de la directiva de Kaspersky Endpoint Security) la notificación del Servidor de administración en las aplicaciones que ejecuta, necesitará gigabytes adicionales (0.03 * C) para almacenar en la base de datos la información sobre las aplicaciones que ejecuta.

Si el Servidor de administración distribuye actualizaciones de Windows (y, por lo tanto, actúa como el servidor de Windows Server Update Services), la base de datos requiere 2.5 GB adicionales.

Durante el funcionamiento, siempre aparece un cierto *espacio no asignado* en la base de datos. Por lo tanto, el tamaño real del archivo de la base de datos (de manera predeterminada, el archivo KAV.MDF si usa SQL Server como DBMS) suele ser aproximadamente el doble del espacio ocupado en la base de datos.

No se recomienda limitar explícitamente el tamaño del registro de transacciones (de forma predeterminada, el archivo KAV_log.LDF, si utiliza SQL Server como DBMS). Se recomienda dejar el valor predeterminado del parámetro MAXSIZE. Sin embargo, si tiene que limitar el tamaño de este archivo, tenga en cuenta que el valor mínimo necesario del parámetro MAXSIZE para KAV_log.LDF suele ser de 20480 MB.

# Calcular el espacio necesario en disco (con y sin el uso de la función Administración de vulnerabilidades y parches)

## Cálculo del espacio necesario en disco si no se usa la función Administración de vulnerabilidades y parches

El espacio en disco que se necesitará aproximadamente para la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit del Servidor de administración se puede calcular con la siguiente fórmula:

(724 * C + 0.15 * E + 0.17 * A), KB

donde:

- C es el número de dispositivos

- E es el número de eventos que se almacenan

- A es el número total de objetos de Active Directory:

  - Cuentas del dispositivo

  - Cuentas de usuario

  - Cuentas de grupos de seguridad

  - Unidades de organización de Active Directory

Si el análisis de Active Directory se encuentra deshabilitado, A se considera igual a cero.

### Cálculo del espacio adicional necesario si se usa la función Administración de vulnerabilidades y parches

- Actualizaciones. La carpeta compartida además requiere al menos 4 GB para almacenar actualizaciones.
- Paquetes de instalación. Si algunos paquetes de instalación se almacenan en el Servidor de administración, la carpeta compartida requerirá una cantidad adicional de espacio libre en disco, igual al tamaño total de todos los paquetes de instalación disponibles para instalar.
- Tareas de instalación remota. Si hay tareas de instalación remotas en el Servidor de administración, se requerirá una cantidad adicional de espacio libre en el disco (en la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit) equivalente al tamaño total de los paquetes de instalación que se instalarán.
- Parches. Si el Servidor de administración se involucra en la instalación de parches, se requerirá una cantidad adicional de espacio de disco:
  - La carpeta de parches debe tener la cantidad de espacio en disco igual al tamaño total de todos los parches que se han descargado. De manera predeterminada, los parches se almacenan en la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles.

    Puede utilizar la utilidad klsrvswch para especificar una carpeta diferente para almacenar parches. La utilidad klsrvswch se encuentra en la carpeta donde está instalado el Servidor de administración. La ruta de instalación predeterminada: <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

    Si el Servidor de administración se utiliza como el servidor de WSUS, le aconsejamos asignar al menos 100 GB a esta carpeta.
  - La carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit debe tener una cantidad de espacio en disco igual al tamaño total de los parches a los que hacen referencia las instancias existentes de las tareas de instalación de actualizaciones (parches) y de reparación de la vulnerabilidad.

## Evaluación del número y configuración de Servidores de administración

Para reducir la carga en el Servidor de administración principal, puede asignar un Servidor de administración separado a cada grupo de administración. El número de Servidores de administración secundarios no puede exceder 500 para un mismo Servidor de administración principal.

Recomendamos que cree la configuración de Servidores de administración en correspondencia con la configuración de la red de su organización.

## Recomendaciones para conectar máquinas virtuales dinámicas a Kaspersky Security Center

Las máquinas virtuales dinámicas (también conocidas como VM dinámicas) consumen más recursos que las máquinas virtuales estáticas.

Para obtener más información sobre las máquinas virtuales dinámicas, consulte Compatibilidad para máquinas virtuales dinámicas.

Cuando se conecta una nueva VM dinámica, Kaspersky Security Center crea un ícono para esa VM dinámica en la Consola de administración y mueve la VM dinámica al grupo de administración. Tras ello, la VM dinámica se agrega a la base de datos del Servidor de administración. El Servidor de administración se sincroniza totalmente con el Agente de red instalado en esta VM dinámica.

En la red de una organización, el Agente de red crea las siguientes listas de red para cada VM dinámica:

- Hardware
- Software instalado
- Vulnerabilidades detectadas
- Eventos y listas de archivos ejecutables del componente Control de aplicaciones

El Agente de red transfiere estas listas de red al Servidor de administración. El tamaño de las listas de red depende de los componentes instalados en la VM dinámica y puede afectar el rendimiento de Kaspersky Security Center y del sistema de administración de bases de datos (DBMS). Tenga en cuenta que la carga puede crecer en forma no lineal.

Una vez que el usuario termina de utilizar y apaga la VM dinámica, la máquina se elimina de la infraestructura virtual y las entradas sobre la VM se eliminan de la base de datos del Servidor de administración.

Todas estas acciones consumen una gran cantidad de recursos de Kaspersky Security Center y de la base de datos del Servidor de administración y pueden, por ende, tener un impacto en el rendimiento de Kaspersky Security Center y del DBMS. No recomendamos conectar más de 20 000 VM dinámicas a Kaspersky Security Center.

Puede conectar más de 20 000 VM dinámicas a Kaspersky Security Center si estas realizan operaciones estándar (por ejemplo, actualizaciones de bases de datos) y consumen, como máximo, un 80 % de la memoria disponible y entre un 75 % y un 80 % de los núcleos disponibles.

El consumo de recursos puede aumentar o disminuir cuando se realizan cambios en la configuración de una directiva, en el software o en el sistema operativo de una VM dinámica. Lo ideal es que se consuma entre un 80 % y un 95 % de los recursos.

# Cálculos para puntos de distribución y puertas de enlace de conexión

Esta sección proporciona los requisitos de hardware para dispositivos utilizados como puntos de distribución junto con recomendaciones para calcular el número de puntos de distribución y puertas de enlace de conexión, según la configuración de la red corporativa.

# Requisitos para un punto de distribución

Para atender hasta 10000 dispositivos cliente, un punto de distribución debe reunir los siguientes requisitos mínimos (la configuración indicada es para un banco de prueba):

- CPU: Intel® Core™ i7-7700, 4 núcleos a 3,60 GHz.
- RAM: 8 GB.
- Espacio de almacenamiento libre: 120 GB.

No se recomienda asignar el Servidor de Administración como punto de distribución, ya que esto aumentará la carga sobre el Servidor de Administración.

Si hay tareas de instalación remota pendientes en el Servidor de administración, el dispositivo que actúa como punto de distribución también debe tener espacio libre suficiente para albergar el tamaño total de los paquetes de instalación que se instalarán.

Si hay una o más instancias de la tarea de instalación de actualizaciones (parches) y reparación de vulnerabilidades pendientes en el Servidor de administración, el dispositivo designado como punto de distribución también debe contar con una cantidad de espacio libre equivalente al doble del tamaño total de todos los parches que se instalarán.

Si utiliza el esquema donde los puntos de distribución reciben las actualizaciones de las bases de datos y los módulos de software de la aplicación directamente de los servidores de actualizaciones de Kaspersky, los puntos de distribución deben estar conectados a Internet.

# Cálculo de la cantidad de puntos de distribución y su configuración

Cuantos más dispositivos cliente contiene una red, más puntos de distribución se requieren. Le recomendamos que no deshabilite la asignación automática de puntos de distribución. Cuando se habilita la asignación automática de puntos de distribución, el Servidor de administración asigna puntos de distribución si el número de dispositivos cliente es bastante grande y define su configuración.

## La utilización de puntos de distribución exclusivamente asignados

Si planea usar ciertos dispositivos específicos como puntos de distribución (es decir, servidores asignados exclusivamente), puede optar por no usar la asignación automática de puntos de distribución. En este caso, compruebe que los dispositivos a los que planea hacer puntos de distribución tengan el volumen suficiente de espacio libre en disco, que no se apaguen con frecuencia y que tengan el modo de suspensión desactivado.

Número de puntos de distribución designados exclusivamente en una red que contiene un único segmento de red, en función del número de dispositivos en red

| Número de dispositivos cliente en el segmento de red | Número de puntos de distribución |
|---|---|
| Menos de 300 | 0 (no corresponde utilizar puntos de distribución) |
| Más de 300 | Aceptable: (N / 10 000 + 1), recomendado: (N / 5000 + 2), donde N es el número de dispositivos conectados a la red |

Número de puntos de distribución designados exclusivamente en una red que contiene múltiples segmentos de red, en función del número de dispositivos en red

| Número de dispositivos cliente por segmento de red | Número de puntos de distribución |
|---|---|
| Menos de 10 | 0 (no corresponde utilizar puntos de distribución) |
| 10–100 | 1 |
| Más de 100 | Aceptable: (N / 10 000 + 1), recomendado: (N / 5000 + 2), donde N es el número de dispositivos conectados a la red |

### Uso de dispositivos cliente estándar (estaciones de trabajo) como puntos de distribución

Si planea usar dispositivos cliente estándar (es decir, estaciones de trabajo) como puntos de distribución, le recomendamos que siga los lineamientos de las siguientes tablas. Al designar los puntos de distribución según estas recomendaciones, evitará las sobrecargas en los canales de comunicación y en el Servidor de administración.

Número de estaciones de trabajo designadas como puntos de distribución en una red que contiene un único segmento de red, en función del número de dispositivos en red

| Número de dispositivos cliente en el segmento de red | Número de puntos de distribución |
|---|---|
| Menos de 300 | 0 (no corresponde utilizar puntos de distribución) |
| Más de 300 | (N / 300 + 1), donde N es el número de dispositivos en red; debe haber al menos 3 puntos de distribución |

Número de estaciones de trabajo designadas como puntos de distribución en una red que contiene múltiples segmentos de red, en función del número de dispositivos en red

| Número de dispositivos cliente por segmento de red | Número de puntos de distribución |
|---|---|
| Menos de 10 | 0 (no corresponde utilizar puntos de distribución) |
| 10–30 | 1 |
| 31–300 | 2 |
| Más de 300 | (N / 300 + 1), donde N es el número de dispositivos en red; debe haber al menos 3 puntos de distribución |

Cuando un punto de distribución se encuentra apagado o no está disponible por algún motivo, los dispositivos administrados en su alcance pueden obtener actualizaciones del Servidor de administración.

## Evaluación del número de pasarelas de conexión

Si planea usar una puerta de enlace de conexión, le recomendamos que designe un dispositivo especial para esta función.

Una puerta de enlace de conexión puede cubrir un máximo de 10 000 dispositivos administrados, incluidos los dispositivos móviles.

# Registro de información sobre eventos para tareas y directivas

Esta sección proporciona evaluaciones asociadas con el almacenamiento de eventos en la base de datos del Servidor de administración y ofrece recomendaciones sobre cómo minimizar el número de eventos, reduciendo así la carga en el Servidor de administración.

De forma predeterminada, en las propiedades de cada tarea y directiva se especifica que todos los eventos asociados con la ejecución de la tarea y la aplicación de la directiva se almacenen en el registro.

Sin embargo, si una tarea se ejecuta con bastante frecuencia (por ejemplo, más de una vez por semana) y en un número bastante grande de dispositivos (por ejemplo, más de 10 000), el número de eventos puede ser demasiado grande y los eventos puede inundar la base de datos. En este caso, se recomienda seleccionar una de dos opciones en la configuración de la tarea:

- **Guardar eventos relacionados con el progreso de la tarea**. En este caso, la base de datos solo recibe información sobre el inicio, el progreso y la finalización de la tarea (satisfactoria, con una advertencia o error) de cada dispositivo en el que se ejecuta.

- **Guardar solo los resultados de la ejecución de la tarea**. En este caso, la base de datos recibe solo información sobre la finalización de la tarea (satisfactoria, con una advertencia o error) de cada dispositivo en el que se ejecuta la tarea.

Si se ha definido una directiva para un número bastante grande de dispositivos (por ejemplo, más de 10 000), el número de eventos también puede ser grande y los eventos pueden inundar la base de datos. En este caso, se recomienda elegir solo los eventos más críticos en la configuración de la directiva y habilitar su registro. Se recomienda desactivar el registro de todos los demás eventos.

Al hacerlo, reducirá la cantidad de eventos en la base de datos, aumentará la velocidad de ejecución de los escenarios asociados con el análisis de la tabla de eventos en la base de datos y disminuirá el riesgo de que una gran cantidad de eventos sobrescriban eventos críticos.

También puede reducir el plazo de almacenamiento para eventos asociados con una tarea o directiva. El período predeterminado es de 7 días para eventos relacionados con tareas y de 30 días para eventos relacionados con directivas. Cuando cambie el plazo de almacenamiento del evento, tenga en cuenta los procedimientos de trabajo establecidos en su organización y la cantidad de tiempo que el administrador del sistema puede dedicar al análisis de cada evento.

Se recomienda modificar la configuración de almacenamiento del evento en cualquiera de los siguientes casos:

- Los eventos referidos a cambios en el estado intermedio de tareas de grupo y los eventos referidos a la aplicación de directivas son un gran porcentaje de todos los eventos en la base de datos de Kaspersky Security Center.

- El registro de eventos de Kaspersky comienza a mostrar entradas sobre la eliminación automática de eventos cuando se excede el límite establecido sobre el número total de eventos almacenados en la base de datos.

Elija las opciones de registro de eventos en el supuesto de que la cantidad óptima de eventos procedentes de un solo dispositivo por día no debe exceder 20. Puede aumentar este límite ligeramente, si es necesario, pero solo si el número de dispositivos en su red es relativamente pequeña (menos de 10 000).

# Consideraciones específicas y configuración óptima de ciertas tareas

Ciertas tareas están sujetas a consideraciones específicas relacionadas con el número de dispositivos en red. Esta sección ofrece recomendaciones sobre la configuración óptima de configuraciones para tales tareas.

El descubrimiento de dispositivos, la tarea de copia de seguridad de datos, la tarea de mantenimiento del Servidor de administración y las tareas de grupo para actualizar Kaspersky Endpoint Security son parte de la funcionalidad básica de Kaspersky Security Center.

## Frecuencia de descubrimiento de dispositivos

No es aconsejable aumentar la frecuencia predeterminada del descubrimiento de dispositivos porque esto puede crear una carga excesiva en los controladores de dominio. En cambio, se recomienda programar el sondeo a la frecuencia mínima posible permitida por las necesidades de su organización. Las recomendaciones para calcular la programación óptima se proporcionan en la tabla a continuación.

Programación para el descubrimiento de dispositivos

| Número de dispositivos en red | Frecuencia recomendada para el descubrimiento de dispositivos |
|---|---|
| Menos de 10000 | Frecuencia predeterminada o menos |
| 10 000 o mayor | Una vez por día o menos |

## Tarea de copia de seguridad de datos del Servidor de administración y tarea de mantenimiento del Servidor de administración

El Servidor de administración deja de funcionar cuando se ejecutan las siguientes tareas:

- Copia de seguridad de los datos del Servidor de administración
- Mantenimiento del Servidor de administración

Cuando se ejecutan estas tareas, la base de datos no puede recibir ningún dato.

Es posible que tenga que reprogramar estas tareas para que no se ejecuten al mismo tiempo que otras tareas del Servidor de administración.

## Tareas de grupo para actualizar Kaspersky Endpoint Security

Si el Servidor de administración actúa como origen de la actualización, la opción de programación recomendada para las tareas de actualización de grupo de Kaspersky Endpoint Security 10 y versiones posteriores es **Al descargar nuevas actualizaciones al repositorio** cuando la casilla **Utilizar retardo aleatorio automático para el inicio de tareas** esté seleccionada.

Si se crea una tarea local para descargar actualizaciones de servidores de Kaspersky al repositorio en cada punto de distribución, la programación periódica es óptima y recomendada para la tarea de actualización del grupo de Kaspersky Endpoint Security. El valor del período de aleatorización debe ser de una hora en este caso.

## Tarea de inventario

Puede reducir la carga a la que se somete la base de datos cuando se obtiene información sobre los archivos ejecutables. Para tal fin, recomendamos que ejecute una tarea de inventario para Kaspersky Endpoint Security en dispositivos de referencia, que tengan instalada una selección de aplicaciones estándar.

El número de archivos ejecutables recibidos por el Servidor de administración desde un único dispositivo no puede ser mayor que 150 000. Cuando Kaspersky Security Center alcanza este límite, no puede recibir ningún archivo nuevo.

Normalmente, el número de archivos en un dispositivo cliente común no supera los 60 000. El número de archivos ejecutables en un servidor de archivos puede ser mayor e incluso superar el umbral de 150 000.

Las mediciones de prueba han demostrado que la tarea de inventario tiene los siguientes resultados en un dispositivo que ejecuta el sistema operativo Windows 7 con Kaspersky Endpoint Security 11 instalado y sin aplicaciones de terceros instaladas:

- Con las casillas de verificación **Inventario de módulos DLL** e **Inventario de archivos Script** desactivadas: aproximadamente 3000 archivos.
- Con el **inventario de módulos DLL** y las casillas de verificación de **Inventario de archivos de script** seleccionadas: de 10 000 a 20 000 archivos, dependiendo de la cantidad de paquetes de servicio del sistema operativo instalados.
- Con solo la casilla de verificación **Inventario de archivos de script** seleccionada: aproximadamente 10 000 archivos.

# Detalles de margen de la carga de la red entre Servidor de administración y dispositivos protegidos

Esta sección proporciona los resultados de las mediciones de prueba del tráfico de red con una descripción de las condiciones bajo las cuales se realizaron las mediciones. Puede consultar esta información cuando planifique la infraestructura de red y la capacidad de rendimiento de los canales de red dentro de su organización (o entre el Servidor de administración y otra organización con dispositivos para proteger). Al conocer la capacidad de rendimiento de la red, también puede estimar aproximadamente cuánto tiempo demorarán las diferentes operaciones de transmisión de datos.

## Consumo de tráfico en diferentes escenarios

La siguiente tabla muestra los resultados de las pruebas de medición realizadas en el tráfico entre el Servidor de administración y un dispositivo administrado en diferentes escenarios.

De forma predeterminada, los dispositivos se sincronizan con el Servidor de administración cada 15 minutos o en un intervalo más largo. Sin embargo, si modifica la configuración de una directiva o tarea en el Servidor de administración la sincronización temprana se produce en los dispositivos a los que se aplica esa directiva/tarea, por lo que las nuevas configuraciones se transmiten a los dispositivos.

Tasa de tráfico entre el Servidor de administración y el dispositivo administrado

| Procedimiento | Tráfico del Servidor de administración hacia cada dispositivo administrado | Tráfico de cada dispositivo administrado al Servidor de administración |
|---|---|---|
| Instalación de Kaspersky Endpoint Security 11.7 para Windows con bases de datos actualizadas | 390 MB | 3.3 MB |
| Instalación del Agente de red | 75 MB | 397 KB |
| Instalación simultánea del Agente de red y Kaspersky Endpoint Security 11.7 para Windows | 459 MB | 3.6 MB |
| Actualización inicial de las bases de datos antivirus sin actualizar las bases de datos incluidas en el paquete (si la participación en Kaspersky Security Network está deshabilitada) | 113 MB | 1.8 MB |
| Actualización diaria de las bases de datos antivirus (si está habilitada la participación en Kaspersky Security Network) | 22 MB | 373 MB |
| Sincronización inicial antes de la actualización de las bases de datos en un dispositivo (transferencia de directivas y tareas) | 382 KB | 446 KB |
| Sincronización inicial después de actualización de bases de datos en un dispositivo | 20 KB | 157 KB |
| Sincronización sin cambios en el Servidor de administración (según el cronograma) | 18 KB | 23 KB |
| Sincronización cuando se cambia una configuración única en una directiva de grupo (tan pronto como se modifique la configuración) | 19 KB | 20 KB |
| Sincronización cuando se cambia una configuración única en una tarea de grupo (tan pronto como se modifique la configuración) | 14 KB | 11 KB |
| Sincronización forzada | 110 KB | 109 KB |
| Evento **del Virus detectado** (1 virus) | 44 KB | 50 KB |
| Evento **del Virus detectado** (10 virus) | 58 KB | 77 KB |
| Tráfico único después de habilitar la lista de registro de aplicaciones | hasta 10 KB | hasta 12 KB |
| Tráfico diario cuando se habilita la lista de registro de aplicaciones | hasta 840 KB | hasta 1 MB |

# Uso promedio de tráfico por 24 horas

El uso promedio de tráfico en 24 horas entre el Servidor de administración y un dispositivo administrado es el siguiente:

- El tráfico del Servidor de administración al dispositivo administrado es de 840 KB.
- El tráfico del dispositivo administrado al Servidor de administración es de 1 MB.

El tráfico se ha medido en las siguientes condiciones:

- Dispositivo administrado con Agente de red y Kaspersky Endpoint Security 11.6 para Windows instalados.
- Ningún punto de distribución asignado al dispositivo.

- La característica Administración de vulnerabilidades y parches no estaba habilitada.
- Frecuencia de sincronización con el Servidor de administración: 15 minutos.

# Contacto con el Servicio de soporte técnico

En esta sección se explica cómo obtener soporte técnico y se describen los términos que rigen este servicio.

## Cómo obtener soporte técnico

Si no encuentra una solución a su problema en la documentación de Kaspersky Security Center o en ninguna de las fuentes de información sobre Kaspersky Security Center, comuníquese con el Servicio de soporte técnico de Kaspersky. Los especialistas del Servicio de soporte técnico responderán a todas sus preguntas acerca de la instalación y el uso de Kaspersky Security Center.

Kaspersky brinda soporte para Kaspersky Security Center durante su ciclo de vida (consulte la página del ciclo de vida de soporte de la aplicación). Antes de comunicarse con el servicio de soporte técnico, lea las reglas de soporte técnico.

Para comunicarse con el servicio de soporte técnico, puede elegir alguna de estas opciones:

- Puede visitar el sitio web del Soporte técnico
- Puede enviar una solicitud al servicio de soporte técnico a través del portal Kaspersky CompanyAccount

## Consultas mediante Kaspersky CompanyAccount al servicio de soporte técnico

Kaspersky CompanyAccount es un portal para empresas que usan aplicaciones de Kaspersky. El portal Kaspersky CompanyAccount está diseñado para que los usuarios puedan comunicarse con los especialistas de Kaspersky fácilmente a través de solicitudes en línea. Puede usar Kaspersky CompanyAccount para seguir el estado de sus solicitudes en línea y también para almacenar un historial de solicitudes.

Puede registrar a todos los empleados de su organización bajo una única cuenta de Kaspersky CompanyAccount. Una cuenta única le permite administrar de forma centralizada las solicitudes electrónicas enviadas a Kaspersky por los empleados registrados y administrar los privilegios de esos empleados a través de Kaspersky CompanyAccount.

El portal Kaspersky CompanyAccount está disponible en los siguientes idiomas:

- Inglés
- Español
- Italiano
- Alemán
- Polaco

- Portugués
- Ruso
- Francés
- Japonés

Para obtener más información sobre Kaspersky CompanyAccount, visite el sitio web del servicio de soporte técnico.

# Obtener archivos de volcado del Servidor de administración

Los archivos de volcado del Servidor de administración contienen toda la información sobre los procesos del Servidor de administración en un determinado momento. Los archivos de volcado del Servidor de administración se almacenan en la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\~dumps. Los archivos de volcado se almacenan mientras Kaspersky Security Center está en uso y se eliminan de forma permanente cuando este elimina. Los archivos de volcado no se envían a Kaspersky automáticamente.

Si el Servidor de administración falla, puede comunicarse con el Servicio de soporte técnico de Kaspersky. Un especialista del Servicio de soporte técnico puede solicitarle que envíe los archivos de volcado del Servidor de administración para su posterior análisis en Kaspersky.

Los archivos de volcado pueden contener datos personales. Antes de enviar información a Kaspersky, recomendamos protegerla contra accesos no autorizados.

# Fuentes de información acerca de la aplicación

## Página de Kaspersky Security Center en el sitio web de Kaspersky

En la página de Kaspersky Security Center en el sitio web de Kaspersky, puede ver información general sobre la aplicación, sus funciones y características.

## Página de Kaspersky Security Center en la Base de conocimientos

La *Base de conocimientos* es una sección del sitio web de soporte técnico de Kaspersky.

En la página de Kaspersky Security Center en la Base de conocimientos, puede leer artículos que proporcionan información útil, recomendaciones, y respuestas a las preguntas más frecuentes sobre cómo comprar, instalar, y utilizar la aplicación.

Los artículos en la Base de conocimiento pueden proporcionar respuestas a preguntas relacionadas tanto con Kaspersky Security Center como con otras aplicaciones de Kaspersky. Estos artículos también pueden contener noticias vinculadas al soporte técnico.

## Discutir las aplicaciones de Kaspersky con la comunidad

Si su pregunta no requiere una respuesta inmediata, puede analizarla con los expertos de Kaspersky y con otros usuarios en nuestro foro.

En el Foro, puede consultar temas de debate, publicar comentarios y crear temas nuevos.

> Se requiere una conexión a Internet para acceder a los recursos web.

Si no encuentra solución a su problema, comuníquese con el servicio de soporte técnico.

# Glosario

## Actualización

Procedimiento de sustitución o adición de nuevos archivos (bases de datos o módulos de software) descargados de los servidores de actualizaciones de Kaspersky.

## Actualización de Kaspersky Security Center

El procedimiento de instalar una nueva versión de Kaspersky Security Center en un dispositivo que tiene instalada una versión anterior de esta aplicación.

## Actualización disponible

Conjunto de actualizaciones para los módulos de una aplicación de Kaspersky. El término incluye las actualizaciones críticas acumuladas durante cierto período de tiempo y aquellas que modifican la arquitectura de la aplicación.

## Administración centralizada de aplicaciones

Administración remota de aplicaciones a través de los servicios disponibles para tal fin en Kaspersky Security Center.

## Administración directa de aplicaciones

Administración de aplicaciones mediante una interfaz local.

## Administrador de Kaspersky Security Center

La persona que administra el funcionamiento de las aplicaciones a través del sistema de administración remota y centralizada Kaspersky Security Center.

## Administrador del cliente

Miembro del personal de una organización cliente que es responsable de supervisar el estado de la protección antivirus.

## Administrador del proveedor de servicios

Un miembro del personal del proveedor de servicios de protección antivirus. Este administrador se encarga de instalar y mantener el sistema de protección antivirus basado en los productos antivirus de Kaspersky y también brinda soporte técnico a los clientes.

## Agente de autenticación

Interfaz que permite autenticarse para obtener acceso a un disco duro cifrado y cargar el sistema operativo si el disco duro de arranque se encuentra cifrado.

## Agente de red

Componente de Kaspersky Security Center que permite la interacción entre el Servidor de administración y las aplicaciones de Kaspersky instaladas en un nodo de red específico (estación de trabajo o servidor). Este componente es el mismo para todas las aplicaciones para Microsoft® Windows® de la empresa. Existen versiones independientes del Agente de red para las aplicaciones de Kaspersky desarrolladas para macOS y sistemas operativos de tipo Unix.

## Aplicación incompatible

Aplicación antivirus que no fue creada por Kaspersky o aplicación de Kaspersky que no se puede administrar a través de Kaspersky Security Center.

## Archivo de clave

Archivo de formato xxxxxxxx.key que hace posible usar una aplicación de Kaspersky con una licencia comercial o de prueba.

## Ataque MITM

Man in The Middle. Ataque a la infraestructura de TI de una organización en el que un hacker se apodera del canal de comunicación entre dos puntos de acceso, lo reencauza y, de ser necesario, cambia la conexión entre estos puntos de acceso.

## Bases de datos antivirus

Bases de datos que contienen información sobre las amenazas a la seguridad informática de las que Kaspersky tiene conocimiento a la fecha de publicarse esas bases de datos. Las entradas de las bases de datos antivirus permiten detectar código malicioso en los objetos analizados. Las bases de datos antivirus son generadas por los especialistas de Kaspersky. Se actualizan cada una hora.

## Brote de virus

Serie de intentos deliberados de infectar un dispositivo con un virus.

## Carpeta Copia de seguridad

Carpeta especial para el almacenamiento de copias de datos del Servidor de administración creadas mediante la utilidad de copia de seguridad.

## Certificado compartido

Certificado que se utiliza para identificar al usuario de un dispositivo móvil.

## Certificado del Servidor de administración

El certificado que utiliza el Servidor de administración para los siguientes fines:

- Autenticación del Servidor de administración al conectarse a la Consola de administración basada en MMC o a Kaspersky Security Center Web Console
- Interacción segura entre el Servidor de administración y los Agentes de red en los dispositivos administrados
- Autenticación de los Servidores de administración al conectar un Servidor de administración principal a un Servidor de administración secundario

El certificado se crea automáticamente cuando se instala el Servidor de administración y queda almacenado en el Servidor de administración.

## Clave activa

Una clave que está siendo utilizada por la aplicación.

## Clave de acceso de AWS IAM

Combinación formada por un id. de clave (una secuencia similar a "AKIAIOSFODNN7EXAMPLE") y una clave secreta (una secuencia similar a "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"). Este par de datos pertenece al usuario de IAM y se usa para obtener acceso a los servicios de AWS.

## Clave de licencia adicional (o de reserva)

Una clave que certifica el derecho a usar la aplicación, pero que no se está utilizando en un momento dado.

## Cliente del Servidor de administración (dispositivo cliente)

Dispositivo, servidor o estación de trabajo que tiene instalado el Agente de red y que tiene aplicaciones de Kaspersky administradas en ejecución.

## Cloud Discovery

Cloud Discovery es un componente de la solución Cloud Access Security Broker (CASB) que protege la infraestructura de la nube de una organización. Cloud Discovery administra el acceso de los usuarios a los servicios en la nube. Los servicios en la nube incluyen, por ejemplo, Microsoft Teams, Salesforce, Microsoft Office 365. Los servicios en la nube se agrupan en categorías, por ejemplo, *Intercambio de datos*, *Mensajería*, *Correo electrónico*.

## Complemento de administración

Componente especializado que proporciona la interfaz para la administración de aplicaciones a través de la Consola de administración. Cada aplicación tiene su complemento. Los complementos de administración vienen incluidos en las aplicaciones de Kaspersky que se pueden administrar mediante Kaspersky Security Center.

## Configuración de la tarea

Ajustes de una aplicación que son específicos para cada tipo de tarea.

## Configuración de programa

Ajustes de una aplicación que son comunes a todos los tipos de tareas y que rigen el funcionamiento general de esa aplicación (esto incluye, por ejemplo, los ajustes relativos al rendimiento, los informes y las copias de seguridad de la aplicación).

## Consola de administración

Un componente de Kaspersky Security Center basado en Windows (también llamado Consola de administración basada en MMC). La Consola de administración proporciona una interfaz de usuario a los servicios de administración del Servidor de administración y del Agente de red.

## Consola de administración de AWS

Interfaz web para ver y administrar los recursos de AWS. La Consola de administración de AWS está disponible en la Web, en https://aws.amazon.com/console/.

## Copia de seguridad de los datos del Servidor de administración

Proceso de copiar los datos del Servidor de administración para crear una versión de respaldo que pueda restaurarse con la utilidad de copia de seguridad. La utilidad puede guardar lo siguiente:

- La base de datos del Servidor de administración (directivas, tareas, configuración de las aplicaciones, eventos guardados en el Servidor de administración)
- Información de configuración relativa a la estructura de grupos de administración y dispositivos cliente
- Repositorio de archivos de instalación para la instalación remota de aplicaciones (el contenido de las carpetas Packages, Uninstall Updates)
- Certificado del Servidor de administración

## Derechos de administrador

Nivel de derechos y privilegios de usuario que se necesitan para administrar objetos de Exchange en una organización de Exchange.

## Directiva

Una directiva determina la configuración de una aplicación y controla la capacidad de configurar esa aplicación en los equipos de un grupo de administración. Se debe crear una directiva individual para cada aplicación. Aunque es posible crear múltiples directivas para las aplicaciones instaladas en los equipos de cada grupo de administración, solamente puede haber una directiva aplicada a cada aplicación dentro de cada grupo de administración.

## Dispositivo con protección de UEFI

Dispositivo que cuenta con una solución o aplicación de Kaspersky para UEFI integrado en el nivel de la BIOS. La protección integrada garantiza que el dispositivo está protegido desde el momento en que se lo enciende. La protección en dispositivos sin software integrado, por el contrario, no comienza a funcionar sino hasta que la aplicación de seguridad se inicia.

## Dispositivo KES

Dispositivo móvil conectado al Servidor de administración de Kaspersky Security Center y administrado a través de la aplicación Kaspersky Endpoint Security para Android.

## Dispositivo MDM con iOS

Dispositivo móvil conectado al Servidor de MDM para iOS mediante el protocolo de MDM para iOS. Los dispositivos que ejecutan el sistema operativo iOS pueden conectarse y administrarse a través del protocolo de MDM para iOS.

## Dispositivos administrados

Dispositivos corporativos que se encuentran conectados a la red y que se han incluido en un grupo de administración.

## Dominio de difusión

Área lógica de una red en la que todos los nodos pueden intercambiar datos, utilizando para ello un canal de difusión en el nivel del modelo OSI (modelo de interconexión de sistemas abiertos).

## Entorno de nube

Máquinas virtuales y otros recursos virtuales desplegados en una plataforma de nube y organizados en redes.

## Estación de trabajo del administrador

Un dispositivo donde se instala la Consola de administración o que use para abrir Kaspersky Security Center Web Console. La Consola de administración es un componente que brinda una interfaz para administrar Kaspersky Security Center.

La estación de trabajo del administrador se utiliza para configurar y administrar el lado del servidor de Kaspersky Security Center. El administrador utiliza esta estación de trabajo para crear y gestionar un sistema de protección antivirus centralizado para una LAN corporativa basado en las aplicaciones de Kaspersky.

## Estado de protección

Estado de protección registrado en un momento dado. Refleja el nivel de seguridad del equipo.

## Estado de protección de la red

Estado de protección registrado en un momento determinado. Define la seguridad de los dispositivos corporativos conectados a la red. Para determinar el estado de protección de la red, se consideran factores como las aplicaciones de seguridad instaladas, el uso de claves de licencia y el número y tipo de amenazas detectadas.

## Función de IAM

Conjunto de derechos para hacer solicitudes a servicios basados en AWS. Las funciones de IAM no están vinculadas a un usuario o grupo específicos; brindan derechos de acceso sin las claves de acceso de AWS IAM. Puede asignar una IAM role a usuarios de IAM , instancias de EC2 y aplicaciones o servicios basados en AWS.

## Gravedad de un evento

Propiedad de un evento registrado durante la ejecución de una aplicación de Kaspersky. Los niveles de gravedad posibles son los siguientes:

- Evento crítico
- Error funcional
- Advertencia
- Información

Dos eventos de un mismo tipo pueden tener niveles de gravedad diferentes si ocurren en situaciones diferentes.

## Grupo de administración

Un conjunto de dispositivos combinados de acuerdo con las funciones que realizan y con las aplicaciones de Kaspersky que tienen instaladas. Los dispositivos se agrupan y se tratan como una sola entidad para facilitar su administración. Cada grupo puede incluir otros grupos. Pueden crearse directivas de grupo y tareas de grupo para cada aplicación instalada en un grupo.

## Grupo de aplicaciones con licencia

Grupo de aplicaciones que el administrador crea sobre la base de distintos criterios (p. ej., por proveedor). El sistema mantiene estadísticas sobre la instalación de las aplicaciones de estos grupos en los dispositivos clientes.

## Guía para reforzar la seguridad

Un conjunto de recomendaciones y funciones para configurar Kaspersky Security Center y sus componentes, con el objetivo de reducir los riesgos de compromiso.

## HTTPS

Protocolo seguro para transferir datos cifrados entre un navegador y un servidor web. HTTPS se usa para obtener acceso a información restringida, como datos corporativos o financieros.

## Identity and Access Management (IAM)

Servicio de AWS que permite gestionar el acceso de los usuarios a otros servicios y recursos de AWS.

## Imagen de máquina de Amazon (AMI)

Plantilla que contiene la configuración de software necesaria para ejecutar una máquina virtual. Cada AMI puede utilizarse para crear más de una instancia.

## Instalación forzada

Método de instalación remota para las aplicaciones de Kaspersky. Permite instalar el software en dispositivos cliente específicos. Para que una instalación forzada se realice correctamente, la cuenta utilizada para la tarea debe tener los derechos necesarios para iniciar aplicaciones de manera remota en los dispositivos cliente. Este método se recomienda para instalar aplicaciones en dispositivos que ejecutan el sistema operativo Windows y admiten esta funcionalidad.

## Instalación local

Método para instalar una aplicación de seguridad en un dispositivo conectado a una red corporativa. El método supone iniciar la instalación manualmente utilizando, o bien el paquete de distribución de la aplicación de seguridad, o bien un paquete de instalación publicado que se haya descargado en el dispositivo de antemano.

## Instalación manual

Instalación de una aplicación de seguridad en un dispositivo de la red corporativa utilizando un paquete de distribución. La instalación manual requiere la participación de un administrador o de otro especialista en TI. Por lo general, la instalación manual se realiza si la instalación remota ha finalizado con errores.

## Instalación remota

Instalación de las aplicaciones de Kaspersky mediante los servicios proporcionados por Kaspersky Security Center.

## Instancia de Amazon EC2

Máquina virtual creada con Amazon Web Services a partir de una imagen AMI.

## Interfaz de programación de aplicaciones de AWS (API de AWS)

La interfaz de programación de aplicaciones que Kaspersky Security Center para la plataforma AWS. Las herramientas de la API de AWS se utilizan, puntualmente, para el sondeo de segmentos de nube y para instalar el Agente de red en las instancias.

## JavaScript

Lenguaje de programación que amplía la funcionalidad de las páginas web. Las páginas web que utilizan JavaScript pueden realizar ciertas funciones (por ejemplo, abrir ventanas adicionales o cambiar la vista de elementos de la interfaz) sin tener que actualizarse con datos nuevos solicitados al servidor web. Para ver páginas con JavaScript, habilite el uso de JavaScript en la configuración de su navegador.

## Kaspersky Private Security Network (KPSN)

Kaspersky Private Security Network es una solución que permite acceder a las bases de datos de reputación de Kaspersky Security Network y a otros datos estadísticos desde un dispositivo sin que se envíen datos a Kaspersky Security Network desde ese dispositivo. Kaspersky Private Security Network está diseñada para clientes corporativos que, por alguno de los siguientes motivos, no pueden participar en Kaspersky Security Network:

- Los dispositivos no tienen acceso a Internet.
- La transmisión de datos fuera del país o de la LAN corporativa está prohibida por ley o por las directivas de seguridad corporativas.

## Kaspersky Security Center System Health Validator (SHV)

Componente de Kaspersky Security Center diseñado para verificar la operatividad del sistema operativo cuando Kaspersky Security Center y Microsoft NAP funcionan simultáneamente.

## Kaspersky Security Network (KSN)

Una infraestructura de servicios en la nube que proporciona acceso a la base de datos de Kaspersky con información constantemente actualizada sobre la reputación de los archivos, recursos web y software. Kaspersky Security Network permite que las aplicaciones de Kaspersky respondan más rápido a las amenazas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de enfrentar falsos positivos.

## Nagent ligero (LWNGT)

Protocolo para la interacción con Kaspersky Endpoint Security en dispositivos móviles. El LWNGT (también llamado protocolo móvil) funciona como Agente de red, pero sin instalar el Agente de red en dispositivos móviles.

## Nivel de importancia del parche

Atributo del parche. Existen cinco niveles de importancia para los parches de Microsoft y los de terceros:

- Crítico
- Alto
- Medio
- Bajo
- Desconocido

El nivel de importancia de un parche de terceros o de Microsoft está determinado por el nivel de gravedad menos favorable entre las vulnerabilidades que el parche debe reparar.

## Operador de Kaspersky Security Center

Usuario que supervisa el estado y el funcionamiento de un sistema de protección administrado mediante Kaspersky Security Center.

## Paquete de instalación

Conjunto de archivos que se crea para instalar una aplicación de Kaspersky de manera remota, mediante el sistema de administración a distancia Kaspersky Security Center. El paquete de instalación contiene una serie de ajustes que se necesitan para instalar la aplicación y ejecutarla inmediatamente una vez que concluye la instalación. La aplicación se configura con los ajustes predeterminados. El paquete de instalación se crea usando archivos con las extensiones .kpd y .kud que vienen incluidos en el kit de distribución de la aplicación.

## Perfil de aprovisionamiento

Conjunto de ajustes para el funcionamiento de una aplicación en un dispositivo móvil iOS. Un perfil de aprovisionamiento contiene información sobre la licencia; está vinculado a una aplicación específica.

## Perfil de configuración

Directiva que contiene un conjunto de ajustes y restricciones para un dispositivo móvil MDM con iOS.

## Perfil de MDM para iOS

Conjunto de ajustes para conectar un dispositivo móvil iOS al Servidor de administración. El dispositivo móvil se conecta al Servidor de administración luego de que el usuario instala un perfil de MDM para iOS en dicho dispositivo.

## Periodo de vigencia de la licencia

Periodo de tiempo durante el cual se tiene acceso a las funciones de la aplicación y a otros servicios adicionales. Los servicios disponibles dependen del tipo de licencia.

## Propietario del dispositivo

El usuario con el que el administrador puede comunicarse cuando surge la necesidad de realizar determinadas operaciones con un dispositivo.

## Protección antivirus para redes

Conjunto de medidas técnicas y organizacionales que disminuyen el riesgo de permitir el ingreso de virus y spam en la red de una organización y que brindan protección contra los ataques de red, el phishing y otras amenazas. La seguridad de una red aumenta cuando se utilizan aplicaciones y servicios de seguridad, y cuando existe y se hace cumplir una política corporativa que regula la seguridad de los datos.

## Proveedor de servicios de protección antivirus

Organización que utiliza las soluciones de Kaspersky para brindarle servicios de protección antivirus a una organización cliente.

## Puerta de enlace de conexión

Una *puerta de enlace de conexión* es un Agente de red que opera de un modo especial. Las puertas de enlace de conexión aceptan conexiones de otros agentes de red y las hacen llegar al Servidor de administración a través de la conexión que mantiene con el mismo. A diferencia de un Agente de red normal, una puerta de enlace de conexión no se encarga de establecer conexión con el Servidor de administración, sino que espera a que el Servidor de administración se conecte a ella.

## Punto de distribución

Equipo en el que se ha instalado el Agente de red y que se utiliza para distribuir actualizaciones, realizar sondeos de red, instalar aplicaciones en forma remota y recopilar información sobre los equipos asociados a un grupo de administración o a un dominio de difusión. Los puntos de distribución están diseñados para optimizar el tráfico de red y reducir la carga del Servidor de administración durante la distribución de actualizaciones. Los puntos de distribución pueden ser designados en forma manual por el administrador o de manera automática por el Servidor de administración. En versiones anteriores de la aplicación, los puntos de distribución se denominaban "agentes de actualización".

## Repositorio de eventos

Una parte de la base de datos del Servidor de administración que se utiliza para almacenar información sobre los eventos ocurridos en Kaspersky Security Center.

## Restauración

Proceso de tomar un objeto original de Cuarentena o Copia de seguridad y colocarlo en su carpeta de origen (la carpeta en la que el objeto se encontraba antes ser desinfectado, eliminado o puesto en cuarentena) o en una carpeta elegida por el usuario.

## Restauración de los datos del Servidor de administración

Restauración de los datos del Servidor de administración a partir de la información guardada en "Copia de seguridad" mediante la utilidad de copia de seguridad. La utilidad puede restaurar lo siguiente:

- La base de datos del Servidor de administración (directivas, tareas, configuración de las aplicaciones, eventos guardados en el Servidor de administración)
- Información de configuración relativa a la estructura de grupos de administración y dispositivos cliente
- Repositorio de archivos de instalación para la instalación remota de aplicaciones (el contenido de las carpetas Packages, Uninstall Updates)
- Certificado del Servidor de administración

## Servidor de administración

Componente de Kaspersky Security Center que almacena centralmente información sobre las aplicaciones de Kaspersky instaladas en la red corporativa. También puede utilizarse para administrar esas aplicaciones.

## Servidor de administración doméstico

El Servidor de administración especificado durante la instalación del Agente de red. El Servidor de administración doméstico puede usarse en la configuración de los perfiles de conexión del Agente de red.

## Servidor de administración virtual

Componente de Kaspersky Security Center diseñado para administrar el sistema de protección de la red de una organización cliente.

El Servidor de administración virtual es una clase particular de Servidor de administración secundario. En comparación con un Servidor de administración físico, los servidores de administración virtuales tienen las siguientes restricciones:

- El Servidor de administración virtual puede crearse solamente en un Servidor de administración principal.
- El Servidor de administración virtual usa la base de datos del Servidor de administración principal. Los servidores de administración virtuales no son compatibles con la tarea de copia de seguridad y restauración de datos ni con la tarea de búsqueda y descarga de actualizaciones.
- El Servidor virtual no admite la creación de Servidores de administración secundarios (incluidos Servidores virtuales).

## Servidor de dispositivos móviles

Componente de Kaspersky Security Center que proporciona acceso a dispositivos móviles y permite administrarlos con la Consola de administración.

## Servidor de MDM para iOS

Componente de Kaspersky Security Center instalado en un dispositivo cliente que permite la conexión de dispositivos móviles iOS al Servidor de administración y la administración de dispositivos móviles iOS por medio del servicio Apple Push Notifications (APNs).

## Servidor web de Kaspersky Security Center

Componente de Kaspersky Security Center que se instala junto con el Servidor de administración. El Servidor web está diseñado para transmitir paquetes de instalación independientes, perfiles de MDM para iOS y archivos de una carpeta compartida a través de una red.

## Servidores de actualizaciones de Kaspersky

Servidores HTTP(S) de Kaspersky desde los que las aplicaciones de Kaspersky descargan actualizaciones para sus bases de datos y módulos de software.

## SSL

Protocolo de cifrado de datos que se usa tanto en redes locales como en Internet. El protocolo SSL se utiliza en aplicaciones web para crear una conexión segura entre el cliente y el servidor.

## Subred de reconocimiento de ubicación de red (NLA)

Servicio de Windows que ayuda al sistema operativo a identificar la red a la que está conectado. NLA detecta cambios en la red y ajusta la configuración de seguridad del dispositivo.

## Tarea

Las funciones que realiza la aplicación de Kaspersky se implementan en forma de tareas. Algunas de estas tareas son Protección de archivos en tiempo real, Análisis completo del equipo y Actualización de las bases de datos.

## Tarea de grupo

Tarea que se define para un grupo de administración y se ejecuta en todos los dispositivos cliente de ese grupo.

## Tarea local

Una tarea definida y ejecutada en un solo equipo cliente.

## Tarea para dispositivos específicos

Tarea asignada a un conjunto de dispositivos cliente tomados de grupos de administración arbitrarios y realizada en dichos dispositivos.

## Tienda de aplicaciones

Uno de los componentes de Kaspersky Security Center. La Tienda de aplicaciones se utiliza para instalar aplicaciones en los dispositivos Android que pertenecen a los usuarios. La Tienda permite publicar los archivos APK de las aplicaciones y vínculos para acceder a las aplicaciones disponibles en Google Play.

## Umbral de actividad viral

Cantidad máxima de eventos de un mismo tipo que se considera admisible en un tiempo limitado. Cuando se supera esta cantidad, se considera que ha habido un aumento en la actividad viral y que se corre el riesgo de enfrentar un brote de virus. Esta característica es importante durante los períodos de brotes de virus puesto que permite que los administradores respondan a tiempo a la amenaza de un ataque de virus.

## Usuario de IAM

Usuario de servicios AWS. Un usuario de IAM puede tener derechos para sondear segmentos de nube.

## Usuarios internos

Las cuentas de usuarios internos se utilizan para trabajar con servidores de administración virtuales. Kaspersky Security Center otorga los permisos de usuarios reales a los usuarios internos de la aplicación.

Las cuentas de los usuarios internos se crean y utilizan solo para trabajar dentro de Kaspersky Security Center. No se transfiere ningún dato sobre estos usuarios internos al sistema operativo. Kaspersky Security Center se encarga de autenticar a los usuarios internos.

## Vulnerabilidad

Error en un sistema operativo o en una aplicación que cualquier creador de malware puede aprovechar para penetrar en el sistema operativo o la aplicación y dañar su integridad. La presencia de una gran cantidad de vulnerabilidades en un sistema operativo lo hace poco confiable, ya que los virus que ingresan al sistema operativo pueden causar alteraciones tanto en el propio sistema operativo como en las aplicaciones instaladas.

## Windows Server Update Services (WSUS)

Aplicación que se utiliza para distribuir actualizaciones para las aplicaciones de Microsoft a los equipos de los usuarios en la red de una organización.

## Zona desmilitarizada (DMZ)

Segmento de una red local en la que hay servidores que atienden solicitudes provenientes de la Web global. El acceso desde la zona desmilitarizada a la red local de la organización se protege con un firewall para garantizar la seguridad de la LAN.

# Información sobre el código de terceros

La información sobre el código de terceros se encuentra en el archivo legal_notices.txt, en la carpeta de instalación de la aplicación.

# Avisos de marcas registradas

Las marcas registradas y las marcas de servicio son propiedad de sus respectivos dueños.

Adobe, Acrobat, Flash, Shockwave y PostScript son marcas registradas o marcas comerciales de Adobe en los Estados Unidos y/o en otros países.

AMD y AMD64 son marcas comerciales o marcas registradas de Advanced Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2 y AWS Marketplace son marcas registradas de Amazon.com, Inc. o de sus empresas vinculadas.

Apache es una marca comercial registrada o una marca comercial de Apache Software Foundation en los Estados Unidos o en otros países.

Apple, AirPlay, AirDrop, AirPrint, App Store, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iCloud, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime y Touch ID son marcas comerciales de Apple Inc.

Arm es una marca registrada de Arm Limited (o de sus filiales) en los EE. UU. y/o en otros lugares.

La palabra, la marca y los logotipos de Bluetooth son propiedad de Bluetooth SIG, Inc.

Ubuntu y LTS son marcas comerciales registradas de Canonical Ltd.

Cisco Systems, Cisco, Cisco Jabber e IOS son marcas comerciales registradas o marcas comerciales de Cisco Systems, Inc. y/o de sus empresas vinculadas en los Estados Unidos y en algunos otros países.

Citrix, XenServer son marcas comerciales o marcas comerciales registradas de Cloud Software Group, Inc. y/o sus filiales en los Estados Unidos y/u otros países.

Corel es una marca comercial o una marca comercial registrada de Corel Corporation y/o de sus filiales en Canadá, los Estados Unidos y/u otros países.

Cloudflare, el logotipo de Cloudflare y Cloudflare Workers son marcas comerciales o marcas comerciales registradas de Cloudflare, Inc. en los Estados Unidos y otras jurisdicciones.

Dropbox es una marca registrada de Dropbox, Inc.

Radmin es una marca comercial registrada de Famatech.

Firebird es una marca registrada de Firebird Foundation.

Foxit es una marca registrada de Foxit Corporation.

FreeBSD es una marca registrada de The FreeBSD Foundation.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Hangouts, Google Public DNS y YouTube son marcas comerciales de Google LLC.

EulerOS, FusionCompute y FusionSphere son marcas comerciales de Huawei Technologies Co., Ltd.

Intel, Core, Xeon son marcas comerciales de Intel Corporation o sus subsidiarias.

IBM y QRadar son marcas comerciales de International Business Machines Corporation y están registradas en muchas jurisdicciones del mundo.

Node.js es una marca registrada de Joyent, Inc.

Linux es una marca registrada de Linus Torvalds en los Estados Unidos y en otros países.

Logitech es una marca comercial registrada o una marca comercial de Logitech en los Estados Unidos y/o en otros países.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, Office 365, PowerShell, PowerPoint, SharePoint, SQL Server, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Mobile, Windows Server, Windows Phone, Windows Vista y Windows Azure son marcas comerciales del grupo de empresas Microsoft.

CVE es una marca registrada de The MITRE Corporation.

Mozilla, Firefox y Thunderbird son marcas comerciales de la Fundación Mozilla en los Estados Unidos y en otros países.

Novell es una marca registrada de Novell Enterprises Inc. en los Estados Unidos y en otros países.

NetWare es una marca registrada de Novell Inc. en los Estados Unidos y en otros países.

OpenVPN es una marca registrada de OpenVPN, Inc.

OpenSSL es una marca comercial de OpenSSL Software Foundation.

Oracle, Java, JavaScript y TouchDown son marcas registradas de Oracle o de sus empresas vinculadas.

Parallels, el logotipo de Parallels y Coherence son marcas comerciales o marcas comerciales registradas de Parallels International GmbH.

Chef es una marca comercial o una marca comercial registrada de Progress Software Corporation y/o una de sus subsidiarias o afiliadas en los EE. UU. y/o en otros países.

Puppet es una marca comercial o una marca comercial registrada de Puppet, Inc.

Python es una marca comercial o una marca comercial registrada de Python Software Foundation.

Red Hat, Fedora y Red Hat Enterprise Linux son marcas comerciales o marcas registradas de Red Hat, Inc. o sus filiales en Estados Unidos y otros países.

Ansible es una marca registrada de Red Hat Inc. en los Estados Unidos y en otros países.

CentOS es una marca comercial o una marca registrada de Red Hat, Inc. o sus filiales en Estados Unidos y otros países.

BlackBerry es propiedad de Research In Motion Limited y está registrada en los Estados Unidos y puede estar pendiente o registrada en otros países.

Rocky Linux es una marca registrada de The Rocky Enterprise Software Foundation.

SAMSUNG es una marca comercial de SAMSUNG en los Estados Unidos o en otros países.

Debian es una marca registrada de Software in the Public Interest, Inc.

Splunk y SPL son marcas comerciales y marcas comerciales registradas de Splunk Inc. en los Estados Unidos y en otros países.

SUSE es una marca registrada de SUSE LLC en los Estados Unidos y en otros países.

La marca Symbian es propiedad de Symbian Foundation Ltd.

OpenAPI es una marca de The Linux Foundation.

UNIX es una marca registrada en los Estados Unidos y en otros países, licenciada exclusivamente a través de X/Open Company Limited.

Zabbix es una marca registrada de Zabbix SIA.

# Problemas conocidos

Kaspersky Security Center Web Console tiene una serie de limitaciones que no son críticas para el funcionamiento de la aplicación:

- La consola muestra la subsección **Alertas** en la sección **Supervisión e informes** del menú principal solo si agregó una clave de licencia para EDR Optimum al repositorio del Servidor de administración ingresando el código de activación.

- Para garantizar la fortaleza del cifrado, el certificado del Servidor de administración debe estar firmado mediante SHA-2 y tener una longitud de clave mínima de 2048. Si necesita volver a emitir el certificado, consulte la Base https://support.kaspersky.com/ksc/15.1/troubleshooting/other/15964#block8 de conocimientos de Kaspersky Security Center.

- Si crea una tarea con la configuración de programación **Cada N días** y **Por días de la semana** en Kaspersky Security Center Linux 15.1 Web Console y luego abre la tarea en versiones anteriores de Kaspersky Security Center Web Console o en la consola de administracion de Kaspersky Security Center Linux (por ejemplo, cuando la tarea también se aplica en los Servidores de administración secundarios, que pueden estar operar tanto en Linux como en Windows), es posible que la configuración de programación se muestre incorrectamente o que se produzca un error.

- Cuando configura la exportación a sistemas SIEM en Kaspersky Security Center Web Console y selecciona el protocolo UDP, se devuelve un error después de hacer clic en el botón **Verificar conexión**, ya que no se establece una conexión mediante UDP y no se puede garantizar la entrega de datos.

- Cuando ejecuta una tarea para eliminar el Agente de red de un dispositivo basado en la arquitectura de Arm y ejecuta Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.7), el Agente de red se elimina correctamente, pero el estado de la tarea para el progreso actual en la lista de tareas se congela.

- La ventana de propiedades de la directiva Kaspersky Device Management para iOS aún contiene la sección **Configuración de dispositivos EAS**, aunque Exchange ActiveSync ya no es compatible.

- La conexión a KSN a través de HTTPS falla si Kaspersky Security Center está instalado en un dispositivo que contiene símbolos cirílicos en el nombre del dispositivo y el proxy de KSN está habilitado en el Servidor de administración.

- Cuando intenta cambiar las propiedades de una cuenta de usuario que tiene habilitada la opción **Solicitar autenticación para verificar el permiso de modificación de cuentas de usuario** y, luego, hace clic en **Cancelar** en la ventana **Protección de cuentas**, se produce un error inesperado.

- Si cambia la hora o la zona horaria en su dispositivo, deberá reiniciar el servicio de Kaspersky Security Center Web Console.

- Si se utiliza un proxy en el dispositivo y se configuran las variables del entorno del proxy, el instalador de Kaspersky Security Center Web Console puede bloquearse.

- Cuando importa la tarea *Descargar actualizaciones a los repositorios de puntos de distribución* o *Verificación de actualizaciones*, se habilita la opción **Seleccionar dispositivos a los que se asignará la tarea**. Estas tareas no se pueden asignar a una selección de dispositivos o a dispositivos específicos. Si asigna la tarea *Descargar actualizaciones a los repositorios de puntos de distribución* o *Verificación de actualizaciones* a dispositivos específicos, la tarea se importará incorrectamente.

- Si realiza el sondeo de Active Directory mediante un punto de distribución de Linux con la versión 15 del Agente de red instalada, puede sondear solo los dominios de Active Directory para los que especifique la dirección y las credenciales de usuario. El sondeo del dominio de Active Directory actual y el bosque de dominios de Active Directory no está disponibles.

- Es posible que no se encuentren los dispositivos cliente después de ejecutar el sondeo de red de Windows.

- El asistente **Agregar un Servidor de administración secundario** finaliza con un error si, para la autenticación en el futuro Servidor secundario, se especifica una cuenta para la que se habilitó la verificación en dos pasos. Para resolver este problema, especifique una cuenta para la que no se encuentre habilitada la función de verificación en dos pasos o cree la jerarquía desde el futuro Servidor secundario.

- Al iniciar sesión en Kaspersky Security Center Web Console, si opta por usar la autenticación de dominio y elige conectarse a un Servidor de administración virtual, cierra luego la sesión y, posteriormente, intenta iniciar sesión en el Servidor de administración principal, Kaspersky Security Center 14 Web Console se conectará al Servidor de administración virtual. Para conectarse al Servidor de administración principal, deberá volver a abrir el navegador.

- El sondeo de red de Windows rápido/completo devuelve un resultado vacío.

- Si instala Kaspersky Security Center Web Console con Identity and Access Manager y luego cambia el Servidor de administración para Kaspersky Security Center Web Console, Identity and Access Manager no obtiene la información sobre el nuevo Servidor de administración.

- Un dispositivo administrado que tiene más de un adaptador de red envía al Servidor de administración información sobre la dirección MAC del adaptador de red que no se ha utilizado para conectarse al Servidor de administración.

- La conexión de prueba a SIEM falla cuando se selecciona el formato de datos CEF.

- La autenticación de NTLM no funciona para cuentas de usuario dentro del grupo Usuarios protegidos.